1.3.9 Prove that if \( n > 1 \) and \( a > 0 \) are integers and \( d = (a, n) \), then the additive order of \( a \) modulo \( n \) is \( n/d \).

Solution: Recall from problem 7 that the additive order of \( a \) modulo \( n \) is the least integer \( x > 0 \) such that \( ax \equiv 0 \pmod{n} \). By Theorem 1.3.5, this equation has a solution since \( \gcd(a, n) \mid 0 \). Moreover, all values of \( x \) satisfying this congruence are congruent modulo \( n/d \). Thus, there is some integer \( r \) such that \( x \equiv r \pmod{n/d} \). Note that \( x = 0 \) is a solution to the original congruence \( ax \equiv 0 \pmod{n} \), so in fact \( r \equiv 0 \pmod{n/d} \). Thus, \( ax \equiv 0 \pmod{n} \) if and only if \( x \equiv 0 \pmod{n/d} \), i.e., if and only if \( (n/d) \mid x \). Finally, the least positive integer that is a multiple of \( n/d \) is just \( n/d \) itself.

Alternate solution: Write \( a = dh \) and \( n = dq \). Then \( ax \equiv 0 \pmod{n} \) if and only if \( n \mid ax \), that is, \( dq \mid dhx \). This happens if and only if \( q \mid hx \). By problem 1.2.8 on the previous homework, \( \gcd(h, q) = 1 \). (That is, once you pull out the gcd, whatever’s left is relatively prime.) Since \( q \mid hx \) if and only if \( q \mid \gcd(h, q)x \), we find \( q \mid hx \) if and only if \( q \mid x \). Unpacking the chain of “if and only if’s” and recalling that \( q = n/d \), we find that \( ax \equiv 0 \pmod{n} \) if and only if \( n/d \mid x \). As before, this shows that \( x = n/d \) is the least positive solution, hence it is the additive order.

1.3.24 Show that the remainder of an integer \( n \) when divided by 9 is the same as the remainder of the sum of its digits when divided by 9.

Solution: Suppose that \( n \) is a positive integer. Then the decimal expansion of \( n \) corresponds to a representation

\[
n = \sum_{i=0}^{N} c_i 10^i,
\]

where each \( c_i \in \{0, 1, \ldots, 9\} \) is a “digit.” To show that \( n \) and the sum of its digits have the same remainder when divided by 9, we want to show that

\[
n \equiv \sum_{i=0}^{N} c_i \pmod{9}.
\]

However, note that \( 10 \equiv 1 \pmod{9} \), so that \( 10^i \equiv 1 \pmod{9} \) for each \( i \geq 0 \). Thus, for each \( i \) we have \( c_i 10^i \equiv c_i \pmod{9} \), and it follows that

\[
\sum_{i=0}^{N} c_i 10^i \equiv \sum_{i=0}^{N} c_i \pmod{9},
\]

which implies (1).

1.3.28 Prove that there exist infinitely many prime numbers of the form \( 4m + 3 \) (where \( m \) is an integer).
Solution: We will mimic Euclid’s proof, but we begin with some preliminary observations. First, observe that an integer \( n \) is of the form \( 4m + 3 \) if and only if \( n \equiv 3 \pmod{4} \). Next, note that if \( p \) is a prime, then \( p \not\equiv 0 \pmod{4} \); thus, \( p \equiv 1, 2 \), or \( 3 \pmod{4} \). Finally, we claim that if \( n \) is of the form \( 4m + 3 \), then it has at least one prime factor also of this form. If this were not the case, then we may write the prime factorization of \( n \) as \( n = 2^{\alpha_0} \cdot p_1^{\alpha_1} \cdots p_r^{\alpha_r} \), where \( \alpha_0 \geq 0 \), and \( p_i \equiv 1 \pmod{4} \) and \( \alpha_i \geq 1 \) for \( 1 \leq i \leq r \). Since each \( p_i \equiv 1 \pmod{4} \), we also have \( p_i^{\alpha_i} \equiv 1 \pmod{4} \) for each \( 1 \leq i \leq r \). Thus, \( n \equiv 2^{\alpha_0} \pmod{4} \). Since \( 2^{\alpha_0} \equiv 1, 2 \), or \( 0 \pmod{4} \) (corresponding to \( \alpha_0 = 0 \), \( \alpha_0 = 1 \), and \( \alpha_0 \geq 2 \), respectively), we find that \( n \not\equiv 3 \pmod{4} \). But we assumed that \( n \) was \( 3 \pmod{4} \), so this is a contradiction, and our claim must be true.

We are now ready to mimic Euclid’s proof. Suppose by way of contradiction that there are only finitely many primes of the form \( 4m + 3 \). Call them \( q_1, \ldots, q_r \). Notice that one of these primes will be 3; let’s suppose it’s \( q_1 \). Consider the integer

\[
n = 4q_2 \cdots q_r + 3.
\]

Notice that \( q_1 = 3 \) has been omitted from the product, so that \( 3 \nmid q_2 \cdots q_r \), which implies \( 3 \nmid n \). As \( n \) is of the form \( 4m + 3 \), it has a prime factor also of the form \( 4m + 3 \) by our claim. Since \( 3 \nmid n \), this prime factor must be \( q_i \) for some \( 2 \leq i \leq r \). But \( q_i \mid 4q_2 \cdots q_r \), so \( q_i \mid (n - 4q_2 \cdots q_r) \), i.e. \( q_i \mid 3 \). This implies that \( q_i = 1 \) or \( 3 \), neither of which can hold. This is a contradiction, establishing the result.

1.4.24 Show that if \( p \) is a prime number, the congruence \( x^2 \equiv 1 \pmod{p} \) has only the solutions \( x \equiv 1 \pmod{p} \) and \( x \equiv -1 \pmod{p} \).

Solution: Notice that \( x^2 \equiv 1 \pmod{p} \) if and only if \( x^2 - 1 \equiv 0 \pmod{p} \), which in turn happens if and only if \( p \mid (x^2 - 1) \). But \( x^2 - 1 = (x - 1)(x + 1) \), so by Euclid’s lemma, this in turn happens if and only if \( p \mid (x - 1) \) or \( p \mid (x + 1) \). Translating back to congruences, this is exactly the assertion that either \( x \equiv 1 \pmod{p} \) or \( x \equiv -1 \pmod{p} \).