11. **The Fundamental Theorem of Arithmetic**

Ryan put up a solution to the first homework problem:

**Example:** (Ryan) 252 is E-zone number with 3 different E-prime factorizations:

\[
252 = (2)(126) \\
= (6)(42) \\
= (14)(18).
\]

It is easily seen that 2, 126, 6, 42, 14, and 18 are E-primes since they are twice odd numbers.

In fact, we can use Ryan’s example to give a solution to the second homework problem:

**Example:** 42 is an E-prime and divides \((14)(18)\). However, 42 does not divide 14 or 18.

For the last homework problem, Shaun gave an example of another Mersenne prime:

**Example:** (Shaun) \(2^{13} - 1 = 8191\) is a Mersenne prime.

We now returned to the subject of prime factorization in the integers. Recall we proved that if \(p\) is prime and \(p\) divides \(ab\) then \(p\) divides \(a\) or \(p\) divides \(b\). (Theorem on page 16.) We will need the following strengthening of this theorem:

**Proposition:** Suppose \(p\) is prime and \(a_1, \ldots, a_n\) are any \(n\) integers such that \(p\) divides the product \(a_1a_2\cdots a_n\). Then \(p\) divides \(a_i\) for some \(i\) between 1 and \(n\).

**Proof:** We will prove this by induction on \(n\) (the number of factors). When \(n = 1\), we just have \(p\) divides \(a_1\). Then of course \(p\) divides one of the factors (namely, \(a_1\)). In the case \(n = 2\) we have that \(p\) divides \(a_1a_2\). Then by the theorem mentioned above, we know that \(p\) divides \(a_1\) or \(a_2\). Now let’s do the induction step. Assume we know the statement is true for \(n\) factors. We need to prove the statement for \(n + 1\) factors. That is, if \(p\) divides \(a_1a_2\cdots a_{n+1}\) we need to show that \(p\) divides one of the factors \(a_i\) \((i = 1, \ldots, n + 1)\). Group the first \(n\) factors into one number; i.e., let \(c = a_1a_2\cdots a_n\). Then we have \(p\) divides \(ca_{n+1}\). By the theorem on page 16 again, we know that \(p\) divides \(c\) or \(p\) divides \(a_{n+1}\). If \(p\) divides \(a_{k+1}\), we’re done. If \(p\) divides \(b = a_1\cdots a_n\), we use the induction hypothesis to say that \(p\) must divide one of \(a_1, \ldots, a_n\). \(\square\)

We are now ready to prove one of the most important theorems about the integers:

**The Fundamental Theorem of Arithmetic:** Every integer greater than or equal to two has a unique factorization into prime integers. By the word *unique* we mean the following: If \(n = p_1 \cdots p_k\) and \(n = q_1 \cdots q_{\ell}\) are two prime factorizations of the integer \(n\) then \(s = t\) (that is, the number of prime factors in each factorization is the same) and, after reordering, \(p_1 = q_1, p_2 = q_2, \ldots, p_k = q_k\).

**Proof:** We have already proved that every integer has a prime factorization (section 12). We just need to prove the uniqueness business. To do this properly, we will prove it by induction on the number \(k\) of prime factors in the first factorization. We first do the case \(k = 1\). In this case, \(n = p_1\), so \(n\) is prime. Since \(p_1\) has no other factors other than 1, it is clear that \(q_1 = p_1\). And \(\ell = 1\) as well (that is, the second factorization has only one prime factor too). Now assume that the theorem is true whenever the first factorization has \(k\) prime factors. We now prove it for \(k + 1\) factors: Let \(n = p_1 \cdots p_{k+1}\) and \(n = q_1 \cdots q_{\ell}\).
Clearly \( p_{k+1} \) (being a prime in the first factorization) divides \( n \). Therefore, \( p_{k+1} \) divides \( q_1 \cdots q_e \). Since \( p_{k+1} \) is prime, we know by the proposition above that \( p_{k+1} \) divides \( q_i \) for some \( i \). After reordering the \( q \)’s, we can assume \( p_{k+1} \) divides \( q_\ell \). Now cancel \( p_{k+1} \) and \( q_\ell \)'s from the equation \( p_1 \cdots p_{k+1} = q_1 \cdots q_\ell \), which gives us

\[
p_1 \cdots p_k = q_1 \cdots q_{\ell-1}.
\]

But the first factorization now has only \( k \) prime factors. By our induction assumption, we know that the uniqueness property holds for this factorization. Thus, the number of primes appearing in the factorizations must be equal; i.e., \( k = \ell - 1 \). This then gives us \( k + 1 = \ell \), which is what we wanted. Also by induction, we know we can that \( p_1 = q_1, p_2 = q_2, \ldots , p_k = q_k \). This completes the proof! \( \square \)

We moved on to a new topic: congruences.

**Definition:** Let \( a, b, \) and \( n \) be integers with \( n > 0 \). Then we say \( a \) is congruent to \( b \) modulo \( n \) if \( n \) divides \( a - b \). The notation we use for this is \( a \equiv b \pmod{n} \).

Here are some examples:

**Example:** \( 7 \equiv 4 \pmod{3} \) since \( 3 | (7 - 4) \).

**Example:** \( 12 \equiv 7 \pmod{5} \) since \( 5 | (12 - 7) \).

**Example:** \( 7 \equiv -3 \pmod{5} \) since \( 5 | (7 - (-3)) \).

We made some elementary observations:

- For any integers \( a \) and \( b \), \( a \equiv b \pmod{1} \), since 1 divides \( a - b \).
- \( a \equiv 0 \pmod{n} \) if and only if \( n \) divides \( a \).
- For any integer \( a \) and \( n \geq 1 \), \( a \equiv a \pmod{n} \).

We then proved that congruence modulo \( n \) is symmetric.

**Theorem:** Let \( a, b, n \) be integers with \( n > 0 \). If \( a \equiv b \pmod{n} \) then \( b \equiv a \pmod{n} \).

**Proof:** Since \( a \equiv b \pmod{n} \), we have \( n | (a - b) \). Then certainly \( n | (-1)(a - b) \), so \( n | (b - a) \). Thus, \( b \equiv a \pmod{n} \). \( \square \)

Congruence modulo \( n \) is also transitive, as Lisa A. showed:

**Theorem:** Let \( a, b, n \) be integers with \( n > 0 \). Suppose \( a \equiv b \pmod{n} \) and \( b \equiv c \pmod{n} \). Then \( a \equiv c \pmod{n} \).

**Proof:** (Lisa A.) As \( a \equiv b \pmod{n} \), we have \( n | (a - b) \). This means \( a - b = nx \) for some \( x \in \mathbb{Z} \). Similarly, as \( b \equiv c \pmod{n} \), we have \( b - c = ny \) for some \( y \in \mathbb{Z} \). Solving for \( b \) in each equation, we have \( b = a - nx \) and \( b = c + ny \). Substituting gives \( a - nx = c + ny \), so \( a - c = nx + ny = n(x + y) \). Hence, \( n \) divides \( a - c \) and so \( a \equiv c \pmod{n} \). \( \square \)

Here is another proof which uses work we have done previously: We have \( n | (a - b) \) and \( n | (b - c) \). Therefore, \( n \) divides \( (a - b) + (b - c) = a - c \). (If \( n \) divides two integers, it divides the sum of those two integers.) Consequently, \( a \equiv c \pmod{n} \).

**Homework:** Let \( a, b, x, y, n \) be integers, with \( n \geq 1 \). Suppose \( a \equiv b \pmod{n} \) and \( x \equiv y \pmod{n} \). Must \( a + x \equiv b + y \pmod{n} \)?