Note: My words to work on your own seem to continue to be ignored. At least, don’t make it so obvious! At least, UNDERSTAND WHAT YOU ARE COPYING!!! I know you are copying without really understanding when I see meaningless statements, or incomplete statements, that make sense when one sees the complete form in someone else’s paper. I may not fail you for it, but rest assured that you I am aware of it. My apologies to the few of you who work on their own and don’t allow others to copy from them.

1. Let \( m, n \) be integers, not both 0. Consider the set \( A = \{ mx + ny : x, y \in \mathbb{Z} \} \). Show that this set coincides with the set of all multiples of the greatest common divisor of \( m, n \). That is, if \( d = \gcd(m, n) \), show \( A = \{ kd : k \in \mathbb{Z} \} \).

   **Solution.** By Bezout, there exist integers \( a, b \) such that \( d = am + bn \). For every \( k \in \mathbb{Z} \) we have \( kd = kam + kbn \in A \), proving that the set \( \{ kd : k \in \mathbb{Z} \} \subset A \). But one also has to prove the converse inclusion! Assume now \( x, y \in \mathbb{Z} \). Since \( d|m \) and \( d|n \), there exists integers \( j, \ell \) such that \( m = jd, n = \ell d \), hence \( mx + ny = jdx + \ell dy = (jx + \ell y)d = kd \) with \( k = jx + \ell y \). The converse inclusion follows.

2. If \( a, m \in \mathbb{N} \) and \( \gcd(a, m) = 1 \), then the order of an integer \( a \) modulo \( m \) is the smallest positive integer \( k \) such that \( a^k \equiv 1 \pmod{m} \). Prove: If \( \gcd(a, m) = 1 \) and if \( k \) is the order of \( a \) modulo \( m \), then \( k|\phi(m) \).

   **Hint:** Divide \( \phi(m) \) by \( k \); what can you say about the remainder?

   **Solution.** Since \( \phi(m) \equiv 1 \pmod{m} \) by Euler’s theorem, we must have \( 1 \leq k \leq \phi(m) \). By the division algorithm, we can write \( \phi(m) = kq + r \) for unique integers \( q, r, 0 \leq r < k \). Now, once again by Euler’s theorem, and because \( a^k \equiv 1 \pmod{m} \),

   \[ 1 \equiv a^{\phi(m)} = a^{kq + r} = (a^k)^q a^r \equiv 1^q a^r = a^r \pmod{m}; \]

   i.e., \( a^r \equiv 1 \pmod{m} \). If \( r > 0 \) then \( 1 \leq r < k \), contradicting that \( k \) is the least positive integer such that \( a^k \equiv 1 \pmod{m} \). Thus \( m = 0 \) and \( k|\phi(m) \).

3. Assume \( p \geq 3 \) is prime and that \( p \nmid a \) and \( a \not\equiv 1 \pmod{p} \). Prove:

   \[ \sum_{k=1}^{p-2} a^k = a + a^2 + \cdots + a^{p-2} \equiv -1 \pmod{p}. \]

   (of course, you do not have to prove the equality; that’s just the definition of the summation expression; you only have to prove the congruence.)

   **Solution.** We have \((a - 1)(1 + a + \cdots + a^{p-2}) = a^{p-1} - 1 \equiv 0 \pmod{p} \), the first equality being a College Algebra equality, the last congruence being due to Fermat’s little theorem. Thus

   \[ p|(a - 1)(1 + a + \cdots + a^{p-2}); \]

   since \( p \nmid a - 1 \) (because \( a \not\equiv 1 \pmod{p} \)), \( p|(1 + a + \cdots + a^{p-2}) \), thus \( a + a^2 + \cdots + a^{p-2} \equiv -1 \pmod{p} \).

4. Textbook, Exercise 13.3 (p. 89).

   **Solution.** See the solution to exercise 8 of Homework 2.


   **Solution.** We know that \( a^m + 1 \) is not prime if \( m \) is an odd number \( \geq 3 \) and \( a > 1 \). That is because if \( m = 2k + 1 \) is odd, \( k \geq 1 \), then

   \[ a^m + 1 = (a + 1)(a^{2k} - a^{2k-1} \pm \cdots - a + 1) \]

   and \( 1 < a + 1 < a^n + 1 \), so \( a + 1 \) is a proper factor of \( a^n + 1 \). Assume now \( a^n + 1 \) is prime, \( a \geq 2, n \geq 2 \). By the prime power decomposition, \( n = 2^k r, \) where \( k \geq 0 \) and \( r \) is odd (\( r \) is the product of all the odd prime factors of \( n \)). Then

   \[ a^n + 1 = \left( a^{2^k} \right)^r + 1 \]

   and because \( a^n + 1 \) is prime, the odd number \( r \) cannot be \( \geq 3 \). Thus \( r = 1 \) and \( n = 2^k \) is a power of 2; we must have \( k \geq 1 \) because \( n \geq 2 \).
6. Determine the highest power of 3 dividing 1000!.

**Solution.** 1000! is the product of all numbers from 1 to 1000. Every third number in the list contributes a factor of 3; every ninth number contributes an additional factor, every twenty seventh number one factor more, and so forth. We have:

Multiples of 3: \([1000/3] = 333\).
Multiples of 9: \([1000/9] = 111\).
Multiples of 27: \([1000/27] = 37\).
Multiples of 81: \([1000/81] = 12\).
Multiples of 243: \([1000/243] = 4\).
Multiples of 729: \([1000/729] = 1\).

Adding up we get that the highest power of 3 dividing 1000! is 498.

7. A nice formula involving Euler’s \(\phi\) function is the following: Let \(n \in \mathbb{N}\) and let \(d_1, \ldots, d_r\) be all the positive divisors of \(n\) (1 and \(n\) included). Then

\[
\phi(d_1) + \phi(d_2) + \cdots + \phi(d_r) = n.
\]

For example, if \(n = 60\), then the divisors of \(n\) are 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60. We have,

\[
\begin{align*}
\phi(1) &= 1, & \phi(2) &= 1, & \phi(3) &= 2, & \phi(4) &= 2, & \phi(5) &= 4, & \phi(6) &= 2, & \phi(10) &= 4, \\
\phi(12) &= 4, & \phi(15) &= 8, & \phi(20) &= 8, & \phi(30) &= 8, & \phi(60) &= 16.
\end{align*}
\]

Then

\[
\phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(5) + \phi(6) + \phi(10) + \phi(12) + \phi(15) + \phi(20) + \phi(30) + \phi(60) = 1 + 1 + 2 + 4 + 2 + 4 + 4 + 8 + 8 + 8 + 16 = 60.
\]

Your mission, should you decide to accept it (and I suggest you do) is to fill out the details in the following sketch of a proof, and then write everything out nicely, as if you were writing a number theory textbook. All I care to see are the finished, polished, product. I am also showing you how the proof works for \(n = 60\); that is purely for your information.

Sketch of a proof. For \(i = 1, \ldots, r\), let \(E(d_i) = \{a \in \mathbb{N} : a \leq d_i, \gcd(a, d_i) = 1\}\). Also, for \(i = 1, 2, \ldots, r\) let \(C(d_i) = \{k : 1 \leq k \leq n, \gcd(n, k) = d_i\}\). Let \(m_i\) be the number of elements in \(C(d_i)\); then \(\sum_{i=1}^{r} m_i = n\) (First missing detail: why is this sum equal to \(n\)?)

For the case \(n = 60\) we would have

\[
C(1) = \{1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59\}, \quad m_1 = 16;
\]

\[
C(2) = \{2, 14, 22, 26, 34, 38, 46, 58\}, \quad m_2 = 8; \quad C(3) = \{3, 9, 21, 27, 33, 39, 51, 57\}, \quad m_3 = 8;
\]

\[
C(4) = \{4, 8, 16, 28, 32, 44, 52, 56\}, \quad m_4 = 8; \quad C(5) = \{5, 25, 35, 55\}, \quad m_5 = 4; \quad m(6) = \{6, 18, 42, 54\}, \quad m_6 = 4;
\]

\[
C(10) = \{10, 50\}, \quad m_7 = 2; \quad C(12) = \{12, 24, 36, 48\}, m_8 = 4; \quad C(15) = \{15, 45\}, \quad m_9 = 2;
\]

\[
C(20) = \{20, 40\}, \quad m_{10} = 2; \quad C(30) = \{30\}, \quad m_{11} = 1; \quad C(60) = \{60\}, \quad m_{12} = 1.
\]

Having worked through an example like this one, one wonders whether it is a coincidence that the \(m_i\)'s come out exactly like the \(\phi(d_i)'s\) with \(d/60\).

The proof continues. Then \#\(C(d_i) = \#E(n/d_i)\) (The sets \(C(d_i)\) and \(E(n/d_i)\) have the same number of elements. In fact, the map

\[
b \mapsto d_i b
\]

is one-to-one and onto from \(E(n/d_i)\) to \(C(d_i)\). Missing detail: Show that this map is one-to one and onto. It follows that \#\(C(d_i) = \phi(n/d_i)\), hence \(\sum_{i=1}^{r} \phi(n/d_i) = n\). But \(\sum_{i=1}^{r} \phi(n/d_i) = \sum_{i=1}^{r} \phi(d_i)\) (why?), hence we are done.
Solution. The original version contains some semi-obvious errors in the sketch of a proof. I was made aware of them, but decided to leave them uncorrected anyway for experimental reasons.

Proof. For \( i = 1, \ldots, r \), let \( E(d_i) = \{ a \in \mathbb{N} : a \leq d_i, \gcd(a, d_i) = 1 \} \). Also, for \( i = 1, 2, \ldots, r \) let \( C(d_i) = \{ k : 1 \leq k \leq n, \gcd(n, k) = d_i \} \). Let \( m_i \) be the number of elements in \( C(d_i) \). Then \( \sum_{i=1}^{r} m_i = n \). In fact, if \( 1 \leq k \leq n \), let \( d = \gcd(n, k) \). Then \( d | n \), thus \( d = d_i \) for some \( i \) and \( k \in C(d_i) \). This shows that \( \{1, 2, \ldots, n\} = \bigcup_{i=1}^{r} C(d_i) \). It is also clear that \( C(d_i) \cap C(d_j) = \emptyset \) if \( i \neq j \), hence \( d_i \neq d_j \) (an element \( k \) cannot have two distinct \( \gcd \)'s with \( n \)). Thus

\[
n = \#\{1, 2, \ldots, n\} = \# \left( \bigcup_{i=1}^{r} C(d_i) \right) = \sum_{i=1}^{r} \#C(d_i) = \sum_{i=1}^{r} m_i
\]

as asserted. Let \( i \in \{1, \ldots, r\} \) and let \( b \in E(n/d_i) \), so \( \gcd(b, n/d_i) = 1 \). We claim that then \( d_i b \in C(d_i) \); i.e., \( \gcd(d_i b, n) = 1 \). Clearly \( d_i \) divides both \( d_i b \) and \( n \). Writing \( n = cd_i \), then \( c = n/d_i \) and \( \gcd(b, c) = 1 \). If \( d_i \) is not the greatest common divisor of \( n, d_i b \), there has to exist a prime \( p \) such that \( p | d_i b, p | n \), and \( p \not\mid d_i \). But from \( p | d_i b, p \not\mid d_i \), we conclude \( p | b \); from \( p | n = cd_i \), \( p \not\mid d_i \) that \( p | c \). Thus \( p | b, p | c \), contradicting \( \gcd(b, c) = 1 \). Thus

\[
b \mapsto d_i b
\]

maps \( E(n/d_i) \) into \( C(d_i) \). We prove next that this map is one-to-one and onto. That is is one-to-one is of course obvious (\( d_i \neq 0 \)). If \( k \in C(d_i) \), then \( \gcd(k, n) = d_i \), thus \( d_i \) divides \( k \); thus \( k = d_i b \) for some \( b \in \mathbb{N} \). Now \( \gcd(b/n/d_i) = \gcd(k/d_i, b/d_i) = 1 \). It follows that \( b \in E(n/d_i) \), proving the map is also onto. It follows that \( \#E(n/d_i) = \#C(d_i) = m_i \); that is, \( \phi(n/d_i) \), which by definition is \( \#E(n/d_i) \), equals \( m_i \). Thus \( \sum_{i=1}^{r} \phi(n/d_i) = n \). But \( \sum_{i=1}^{r} \phi(n/d_i) = \sum_{i=1}^{n} \phi(d_i) \) because as \( d \) ranges through the divisors of \( n \), so does \( n/d \); that is

\[
\{d_1, \ldots, d_r\} = \{n/d_1, n/d_2, \ldots, n/d_r\}.
\]

We are done. \( \blacksquare \)