Concepts:

- Define prime and composite numbers.
- Be familiar with the theorem that states that there are infinitely many prime numbers.
- Prove that a small integer is prime by using trial division by increasing primes up to the square root of the integer.
- Determine the unique prime factorization of a given positive integer n, $n \geq 2$.
- Evaluate the gcd and/or lcm of two positive integers using their prime factorization.
- Evaluate the gcd of two positive integers using the Euclidean algorithm.

Problems:

1. Fill in the blanks in the following definitions and theorems:

   (a) An integer number is said to be prime if ...

   (b) The greatest common divisor of two positive integers a and b is the positive integer d such that ...

   (c) The Fundamental Theorem of Arithmetic (unique prime factorization theorem) states that ...

   (d) Two positive integers are said to be relatively prime if ...

   (e) The Euclidean Algorithm is an efficient method to determine ...

2. Check whether the following are true or false. Justify your answer briefly.

   (a) To verify that 139 is prime, we only need to show that 139 is not divisible by 2, 3, 5, 7 and 11.

   (b) Knowing that 5851, 5857, 5861 and 5867 are prime, we can be certain that $5851 \cdot 5867 \neq 5857 \cdot 5861$ without evaluating the two products.

   (c) There is a prime number greater than 10^{100}.

   (d) Prime factorization is computationally more efficient for finding the gcd of two positive integers than the Euclidean Algorithm.

   (e) There are pairs of integers such that their gcd is 52 and their lcm is 520.

3. Let p and q be two distinct prime numbers. List all positive divisors of the integer $n = p^2q^2$.

4. Let p and q be two distinct prime numbers. Determine the number of positive divisors of the integer $n = p^3q^5$.

5. If p, q and r are three distinct prime numbers, how many of the positive divisors of $p^3q^5r^6$ are relatively prime to r^9?

6. The product of two numbers is 48 and their gcd is 2. What is their lcm?

7. Use the Euclidean Algorithm to evaluate the gcd of 1002 and 999.

8. Let us assume that m and b are positive integers such that $12m = 25b$. Prove that that $5|m$.

9. Determine the gcd of $5^2 \cdot 7^6$ and $3 \cdot 5 \cdot 7^9$.

10. Let p be a prime number and a be an arbitrary positive integer. Prove that if $p|a^2$, then $p|a$.

11. For an integer $n \geq 2$, we define $\varphi(n)$ to be the number of integers k, $1 \leq k < n$, that are relatively prime to n.

    (a) Find $\varphi(7)$ and $\varphi(49)$.

    (b) Generalize the idea from part (a) and find a formula for $\varphi(p)$ and $\varphi(p^\alpha)$ for a prime number p and positive integer α.

12. What is the smallest positive integer m such that $3^4 \cdot 7^3 \cdot 11^7 \cdot m$ is a perfect square?

13. What is the smallest positive integer m such that $3^4 \cdot 7^3 \cdot 11^7 \cdot m$ is a cubic number?

14. Let us assume that a and b are positive integers. Prove that $\gcd(a, b) = \mathrm{lcm}(a, b)$ if and only if $a = b$.

Solutions:

1. Fill in the blanks in the following definitions and theorems:

   (a) An integer number is said to be prime if it is greater than or equal to 2 and is divisible only by 1 and the number itself. Equivalently, a prime number is a positive number with exactly two positive divisors.

   (b) The greatest common divisor of two positive integers a and b is the positive integer d such that d is the largest integer that divides both a and b.

   (c) The Fundamental Theorem of Arithmetic (unique prime factorization theorem) states that every integer greater than 1 can be represented uniquely as a product of prime numbers, not considering the order of the factors.

   (d) Two positive integers are said to be relatively prime if the only positive integer that is a divisor of both of them is 1. Equivalently, two positive integers are relatively prime if and only if their gcd equals 1.

   (e) The Euclidean Algorithm is an efficient method to determine the gcd of any two positive integers.

2. Check whether the following are true or false. Justify your answer briefly.

   (a) To verify that 139 is prime, we only need to show that 139 is not divisible by 2, 3, 5, 7 and 11.

   True. Recall that any integer $n \geq 2$ is either prime or it is composite. Also, we know that if n is composite, then there exists a positive divisor of n, say m such that $m \leq \sqrt{n}$. Proof of this fact can be obtained by contradiction. Hence when we check if a number ≥ 2 is prime or not, we need to check only its divisibility by the prime numbers $\leq$ the square root of the number itself.
   Since $11^2 = 121 < 139 < 144 = 12^2$, we assess that $11 < \sqrt{139} < 12$, so all the primes less than $\sqrt{139}$ are $2, 3, 5, 7$, and 11, Thus, the statement is true.

   (b) Knowing that 5851, 5857, 5861 and 5867 are prime, we can be certain that $5851 \cdot 5867 \neq 5857 \cdot 5861$ without evaluating the two products.

   True. To get a contradiction, we assume that $5851 \cdot 5867 = 5857 \cdot 5861 = N$. Relying on the information that the four given numbers are distinct primes, the equality would claim that the integer N has two different prime factorizations, which is not possible by the Fundamental Theorem of Arithmetic.

   (c) There is a prime number greater than 10^{100}.

   True. There are infinitely many prime numbers and there are only finitely many positive integers that are less than or equal to 10^{100}. Thus, there must be infinitely many prime numbers greater than 10^{100}.

   (d) Prime factorization is computationally more efficient for finding the gcd of two positive integers than the Euclidean Algorithm.

   False. The Euclidean Algorithm is computationally much more efficient in finding the gcd of two positive integers than the prime factorization process, especially for larger numbers. No efficient prime factorization algorithm is known for large integers, and with the currently known methods, it would take millions of years to find the prime factorization of large integers. On the other hand, the Euclidean Algorithm has logarithmic complexity.

(e) There are pairs of positive integers such that their gcd is 52 and their lcm is 520.

True. If the $\gcd(a,b) = 52$ for two positive integers a and b, then $a = 52s$ and $b = 52t$ for some positive integers s and t, where $\gcd(s,t) = 1$. Let us substitute $a = 52s$, $b = 52t$ and $\gcd(a,b) = 52$ into the identity $\gcd(a,b) \cdot \operatorname{lcm}(a,b) = a \cdot b$. Then we obtain $52 \cdot \operatorname{lcm}(a,b) = 52^2 st$, which implies $\operatorname{lcm}(a,b) = 52st$ where $\gcd(s,t) = 1$.

Now, we need to find s and t such that $\operatorname{lcm}(a,b) = 52st = 520$. Thus, $st = 10$, which implies $s = 1, t = 10$ or $s = 2$ or $t = 5$ or vice versa. Hence, $a = 52$ and $b = 520$ is one such pair, and the other one is $a = 104$ and $b = 260$.

3. Let p and q be two distinct prime numbers. List all positive divisors of the integer $n = p^2q^2$.

Any integer in the form of $p^i \cdot q^j$, where $i = 0, 1, 2$ and $j = 0, 1, 2$, is a positive divisor of n for any combination of the values of i and j. Thus, the positive divisors of n are: 1, p, p^2, q, pq, p^2q, q^2, pq^2, p^2q^2. Note that there are $3 \cdot 3 = 9$ divisors.

4. Let p and q be two distinct prime numbers. Determine the number of positive divisors of the integer $n = p^3q^5$.

In general, the number of divisors for an integer $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ where p_1, $p_2, \ldots$ p_k are distinct primes, is given by $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$. Hence, n has $(3 + 1)(5 + 1) = 24$ divisors including 1 and n itself.

5. If p, q and r are three distinct prime numbers, how many of the positive divisors of $p^3q^5r^6$ are relatively prime to r^9?

Any divisor in the form of $p^i \cdot q^j$, where $i = 0, 1, 2, 3$ and $j = 0, 1, 2, 3, 4, 5$, is relatively prime to r^9. Thus, there are $4 \cdot 6 = 24$ positive divisors that are relatively prime to r^9.

6. The product of two numbers is 48 and their gcd is 2. What is their lcm?

We know that for any two positive integers a and b,

$$\gcd(a,b) \cdot \operatorname{lcm}(a,b) = a \cdot b.$$

This implies, $\operatorname{lcm}(a,b) = \frac{48}{2} = 24$.

7. Use the Euclidean Algorithm to evaluate the gcd of 1002 and 999.

First we divide 1002 by 999 and use successive divisions to carry out the Euclidean Algorithm. The algorithm stops when the remainder becomes 0. The previous (non-zero) remainder is the gcd.

$$\begin{aligned} 1002 &= 1 \cdot 999 + 3 \\ 999 &= 333 \cdot 3 + 0 \end{aligned}$$

Hence, $\gcd(1002, 999) = 3$.

8. Let us assume that m and b are positive integers such that $12m = 25b$. Prove that $5|m$.

Proof: Consider the equation, $12m = 25b$, which can be rewritten as $12m = 5 \cdot (5b)$. Thus, by the definition of divisibility, $5|12m$. Since 5 is a prime number, $5|12$ or $5|m$. We know that $5 \nmid 12$, and hence $5|m$. ■

9. Determine the gcd of $5^2 \cdot 7^6$ and $3 \cdot 5 \cdot 7^9$?

   To find the greatest common divisor of these two numbers, we take the common prime factors raised to the smaller exponent. Thus, gcd of $5^2 \cdot 7^6$ and $3 \cdot 5 \cdot 7^9$ is $5 \cdot 7^6$.

10. Let p be a prime number and a be an arbitrary positive integer. Prove that if $p|a^2$, then $p|a$.

    Proof: Let the prime factorization of a be as follows: $a = p_1 p_2 \dots p_n$, where $p_1,\ p_2,\ \dots,\ p_n$ are primes that are not necessarily distinct. Therefore, $a^2 = (p_1 p_2 \dots p_n)(p_1 p_2 \dots p_n) = (p_1)^2(p_2)^2 \dots (p_n)^2$.

    Now, we are given that p divides a^2. Therefore, from the Fundamental Theorem of Arithmetic, it follows that p is one of the prime factors of a^2.

    However, the only prime factors of a^2 are $p_1, p_2, \dots p_n$, so p must be one of $p_1,\ p_2, \dots,\ p_n$ by the uniqueness part of the Fundamental Theorem of Arithmetic.

    Since $a = p_1 p_2 \dots p_n$, and p is one of these prime factors, p divides a. ■

11. For an integer $n \geq 2$, we define $\varphi(n)$ to be the number of integers k, $1 \leq k < n$, that are relatively prime to n.

    (a) Find $\varphi(7)$ and $\varphi(49)$.

    Since 7 is a prime number, $1, 2, 3, 4, 5$ and 6 are the positive integers up to 7 that are relatively prime to 7. Hence, $\varphi(7) = 7 - 1 = 6$.

    For $49 = 7^2$, the positive integers that are not relatively prime to 49 are the multiples of 7. Thus, $1 \cdot 7 = 7$, $2 \cdot 7 = 14$, $3 \cdot 7 = 21$, $4 \cdot 7 = 28$, $5 \cdot 7 = 35$, $6 \cdot 7 = 42$ and $7 \cdot 7 = 49$ are exactly the positive non-relative primes to 49, not exceeding 49. Thus, $\varphi(49) = 49 - 7 = 42$.

    (b) Generalize the idea from part (a) and find a formula for $\varphi(p)$ and $\varphi(p^\alpha)$ for a prime number p and positive integer α.

    For a positive prime integer p, the number of integers relatively prime to it are all the integers up to p, not including p. Therefore, $\varphi(p) = p - 1$.

    For p^α, the positive integers that are not relatively prime to p^α, and do not exceed p^α, are multiples of p, i.e., integers in the form of $k \cdot p$ where $k = 1, 2, 3, \dots, p^{\alpha-1}$. Thus, there are $p^{\alpha-1}$ positive integers that are not relatively prime to p^α and not exceeding it. Hence, $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1} \cdot (p-1)$.

    The function φ defined in the statement of this problem is called "*Euler's Totient Function.*"

    For a positive integer n, a general formula for $\varphi(n)$ can be derived. (See Wikipedia for Euler's Totient Function.)

12. What is the smallest positive integer m such that $3^4 \cdot 7^3 \cdot 11^7 \cdot m$ is a perfect square?

    Applying the Fundamental Theorem of Arithmetic, an integer is a perfect square exactly when each prime in its factorization appears an even number of times. Hence $m = 7 \cdot 11$ is the smallest integer.

13. What is the smallest positive integer m such that $3^4 \cdot 7^3 \cdot 11^7 \cdot m$ is a cubic number?

    Applying the Fundamental Theorem of Arithmetic, an integer is a perfect cube exactly when the exponent of each prime factor is a multiple of 3. Hence $m = 3^2 \cdot 11^2$ is the smallest integer.

14. Let us assume that a and b are positive integers. Prove that $\gcd(a, b) = \operatorname{lcm}(a, b)$ if and only if $a = b$.

Proof: If $a = b$, then it is clear that $\gcd(a, b) = \operatorname{lcm}(a, b) = a$. Now we will show that if $\gcd(a, b) = \operatorname{lcm}(a, b)$, then $a = b$.

Let $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ and $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}$ where $p_1,\ p_2,\ \dots,\ p_n$ are distinct primes and α_i's and β_i's are non-negative integers. Since in fact a and b may not have the exact same prime factors (or may have no common primes at all), we relax the condition on exponents from positive integers to non-negative integers for convenience.

Then

$$\begin{aligned}\gcd(a, b) &= p_1^{min(\alpha_1,\beta_1)} \cdot p_2^{min(\alpha_2,\beta_2)} \dots p_n^{min(\alpha_n,\beta_n)}\\ \operatorname{lcm}(a, b) &= p_1^{max(\alpha_1,\beta_1)} \cdot p_2^{max(\alpha_2,\beta_2)} \dots p_n^{max(\alpha_n,\beta_n)}.\end{aligned}$$

Using the Fundamental Theorem of Arithmetic, these last equations, in conjunction with the fact that $\gcd(a, b) = \operatorname{lcm}(a, b)$, we infer that $\max(\alpha_i, \beta_i) = \min(\alpha_i, \beta_i)$, for all $i = 1, 2, \dots \dots n$, Hence $\alpha_i = \beta_i$, for all $i = 1, 2, \dots \dots n$, and, so, $a = b$. ■