Properties of Integers: Divisibility, Primes, Euclid’s Division Algorithm, Greatest Common Divisor (GCD), and Least Common Multiple (LCM)

Recall the following definition of divisibility of integers:

**Definition:** An integer \( a \) is divisible by integer \( b \), where \( b \neq 0 \), if \( a = bc \) for some integer \( c \). In this case, \( b \) is called a divisor of \( a \); the notation is \( b \mid a \). We often restricted the divisors to positive integers since if \( b \mid a \), where \( b \neq 0 \), then \((-b) \mid a\).

For example, since \( 12 = 3 \cdot 4 \), we can say \( 3 \mid 12 \) (and \( 4 \mid 12 \)). Also, \( 1 \mid n \) and \( n \mid n \) for any non-zero integer \( n \).

**Definition:** An integer \( p \) is called a prime if \( p \geq 2 \), and the only (positive) divisors of \( p \) are 1 and \( p \) itself; that is, if \( p \) is a prime and \( a \mid p \), where \( a > 0 \), then \( a = 1 \) or \( a = p \).
Thus, some primes are 2, 3, 5, 7, 11, 13, … It is well known that there exist infinitely many primes (proved by Euclid). However, it is still unknown whether there are infinitely many prime pairs such as 3 and 5, 5 and 7, 11 and 13, etc., where two primes of the form $p$ and $p+2$ (known as twin primes). Any integer $n > 1$ can be factored into a product of primes in essentially a unique way, which is known as the fundamental theorem of arithmetic. It turns out that factorization is not a trivial problem; that is, given a (large) integer finding its factors may take many steps given the state-of-art algorithms. However, finding common factors between two integers can be done very efficiently, something known to Euclid.

**Definition:** Given two positive integers $a$ and $b$. An integer $m$ is a common divisor of $a$ and $b$ if $m | a$ and $m | b$. The greatest common divisor of $a$ and $b$, denoted GCD($a, b$), is the largest of the common divisors of $a$ and $b$. Note that the GCD always exists since 1 is always a common divisor, so GCD($a, b$) ≥ 1. Two integers $a$ and $b$ are relatively prime if GCD($a, b$) = 1.
We now develop Euclid’s algorithm which computes the GCD of two positive integers. The
basic idea is based on the following theorem.

**Theorem:** If \( a = bq + r \), where \( b \neq 0 \), then \( \text{GCD}(a, b) = \text{GCD}(b, r) \).

**Proof:** We first note that if \( m \mid a \) and \( m \mid b \) (that is, if \( m \) is a common divisor of \( a \) and \( b \)), then \( m \mid r \). This is true because \( m \mid a \) implies \( a = mc \); \( m \mid b \) implies \( b = md \), for some integers \( c \) and \( d \). Thus, \( r = a - bq = mc - mdq = m(c - dq) \), which proves \( m \mid r \). Thus, \( m \) is a common divisor of \( b \) and \( r \). Therefore, \( m \leq \text{GCD}(b, r) \) by the definition of \( \text{GCD}(b, r) \). In particular, \( \text{GCD}(a, b) \leq \text{GCD}(b, r) \). Similarly, we can prove that any common divisor of \( b \) and \( r \) divides \( a \). Thus, \( \text{GCD}(b, r) \leq \text{GCD}(a, b) \). Combining the two inequalities proves the theorem.
Example: We now illustrate Euclid’s GCD algorithm by computing GCD(228, 95).

\[ 228 = 95 \cdot 2 + 38, \text{ so } GCD(228, 95) = GCD(95, 38). \]

Repeating the division process, using the previous divisor and remainder as the dividend and divisor, respectively, of the next step, we find

\[ 95 = 38 \cdot 2 + 19, \text{ so } GCD(95, 38) = GCD(38, 19); \text{ and since} \]
\[ 38 = 19 \cdot 2 + 0, \text{ so } GCD(38, 19) = GCD(19, 0) = 19. \]

Combining, we find GCD(228, 95) = 19, the divisor of the last division step.

Note that the above process always terminates since each remainder is strictly smaller than the divisor of that step, thus strictly smaller than the remainder of the previous step, so the remainder eventually becomes zero. When that occurs, the last GCD between the divisor and zero is the divisor itself, which gives the GCD of the original pair of integers.
Euclid’s algorithm written in C that computes the GCD is given below:

```c
int gcd (int a, int b) // assume a, b > 0
{  int r;
    while (1) {// repeat until remainder = 0
        r = a % b; // r is the remainder
        if (r == 0) return b;
        // otherwise
        a = b; b = r;
    }
}
```

**Theorem:** Suppose $a$ and $b$ are two positive integers. There exist integers $t$ and $u$ (may not be positive) such that $at + bu = \text{GCD}(a, b)$. That is, the GCD can be written as a linear combination of the two integers.

We will “demonstrate” this theorem by the extended Euclid’s GCD algorithm. Basically, the GCD is equal to the remainder of the second-to-the-last division step of Euclid’s algorithm. Thus, the GCD can be written as a linear combination of the dividend and the divisor of that division step. We can then use the division step above it to substitute out its remainder, resulting in a linear combination of the dividend and divisor from this previous step. Repeating the substitutions using the division steps toward the beginning of Euclid’s algorithm eventually leads to a linear combination in terms of the original pairs of the integers.
**Example.** Find integers \( t \) and \( u \) such that \( \text{GCD}(228, 95) = 228 \ t + 95 \ u \), that is, write \( \text{GCD}(228, 95) \) as a linear combination of 228 and 95.

Recall the following division steps in computing \( \text{GCD}(228, 95) \) using Euclid’s algorithm:

\[
228 = 95 \cdot 2 + 38 \quad \text{--- (1)}, \quad 95 = 38 \cdot 2 + 19 \quad \text{--- (2)}, \quad \text{and} \quad 38 = 19 \cdot 2 + 0 \quad \text{--- (3)}
\]

Thus, \( \text{GCD}(228, 95) = 19 \), and \( \text{GCD}(228, 95) = 19 = 95 - 38 \cdot 2 \quad \text{--- (4)}, \) by rewriting the remainder in Step (2). We now substitute out the remainder 38 from Step (1), thus, rewriting (4) as

\[
19 = 95 - (228 - 95 \cdot 2) \cdot 2
\]

\[
= 228 \cdot (-2) + 95 \cdot (4 + 1), \quad \text{by combining the like terms, writing as a linear combination}
\]

\[
\text{of the previous dividend and divisor}
\]

\[
= 228 \cdot (-2) + 95 \cdot 5.
\]

Thus, \( t = -2 \) and \( u = 5 \).
**Theorem:** If $p$ is a prime and $p | ab$, then $p | a$ or $p | b$, where $a$ and $b$ are two positive integers.

**Proof:** Consider the value of $\text{GCD}(p, a)$. Since this is a divisor of $p$, but $p$ is a prime by assumption, so $\text{GCD}(p, a) = 1$ or $p$ (by the definition primes). We now have two cases:

(Case one)
Suppose $\text{GCD}(p, a) = 1$. Write $1 = pt + au$ using the Extended Euclid’s algorithm. Multiplying both sides by $b$ yields $b = ptb + abu = p(tb + mu)$ assuming $ab = pm$ since $p | ab$ by assumption. Thus, we proved $p | b$ in this case,

(Case two)
Suppose $\text{GCD}(p, a) = p$. In this case, $p$ is the GCD of $p$ and $a$, so $p | a$. 
We can now state the following theorem which says any integer greater than 1 can be factored into a product of primes, in essentially a unique way. The proof is given on pages 3-6 and 3-7.

**Theorem (Fundamental Theorem of Arithmetic).** Let \( n \geq 2 \) denote an integer. Then there exists prime numbers \( p_1, p_2, \ldots, p_k \), not necessarily distinct, such that \( n = p_1 p_2 \ldots p_k \); that is, any integer \( n \geq 2 \) can be factored as a product of prime numbers. Furthermore, the product is unique except for possible rearrangement of the prime factors.

**Example.** Consider the following prime factorizations:

\[
10296 = 2^3 \cdot 3^2 \cdot 11 \cdot 13; \quad 12675 = 3 \cdot 5^2 \cdot 13^2; \quad \text{and} \quad 25168 = 2^4 \cdot 11^2 \cdot 13.
\]

Note that the GCD can be calculated quickly once the prime factorizations are given. That is, if integers \( a \) and \( b \) have a common prime factor \( p \), e.g., \( p^\alpha \mid a \) and \( p^\beta \mid b \), then \( p^{\min(\alpha, \beta)} \) is a prime-power factor in \( \gcd(a, b) \). Thus,

\[
\gcd(10296, 12675) = 3 \cdot 13 = 39; \quad \text{and} \quad \gcd(10296, 25168) = 2^3 \cdot 11 \cdot 13 = 1144.
\]
**Definition:** The least common multiple of two integers $a$ and $b$, denoted $\text{LCM}(a, b)$, is the smallest positive multiple of $a$ and $b$. For example, $\text{LCM}(10296, 12675) = 2^3 \cdot 3^2 \cdot 5^2 \cdot 11 \cdot 13^2$ and $\text{LCM}(10296, 25168) = 2^4 \cdot 3^2 \cdot 11^2 \cdot 13$.

**Theorem:** $\text{GCD}(a, b) \cdot \text{LCM}(a, b) = ab$, for any two positive integers $a$ and $b$.

**Proof:** It can be seen that if $p^\alpha \mid a$ and $p^\beta \mid b$, then $p^{\max(\alpha, \beta)}$ is a prime-power factor in $\text{LCM}(a, b)$. Thus, the prime-power factor using prime $p$ in $\text{GCD}(a, b) \cdot \text{LCM}(a, b)$ is $p^{\min(\alpha, \beta)} \cdot p^{\max(\alpha, \beta)}$ which equals $p^{\alpha + \beta}$, exactly the same as the prime-power factor using prime $p$ in $ab$. Since this is true for all prime-power factors of $a$ and $b$, the theorem is proved.