Primes and Greatest Common Divisors

Primes

An integer *p* greater than 1 is called *prime* if the only positive factors of *p* are 1 and *p*.

Composite

A positive integer that is greater than 1 and is not prime is called *composite*

Remark: The integer *n* is composite if and only if there exists an integer $a \neq 0$ such that $a \mid n$ and $1 < a < n$.

THE FUNDAMENTAL THEOREM OF ARITHMETIC

THEOREM 1

Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

Example

The prime factorizations of 100, 641, 999, and 1024 are given by

$$\begin{aligned}
100 &= 2 * 2 * 5 * 5 = 2^2 5^2, \\
641 &= 641, \\
999 &= 3 * 3 * 3 * 37 = 3^3 * 37, \\
1024 &= 2 * 2 * 2 * 2 * 2 * 2 * 2 * 2 * 2 * 2 = 2^{10}
\end{aligned}$$

- **THEOREM 2** If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

Proof: If n is composite, by the definition of a composite integer, we know that it has a factor a with $1 < a < n$.

Hence, by the definition of a factor of a positive integer, we have $n = ab$, where b is a positive integer greater than 1.

We will show that $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. If $a > \sqrt{n}$ and $b > \sqrt{n}$,

then $ab > \sqrt{n} \cdot \sqrt{n} = n$, which is a contradiction.

Consequently, $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.
Because both a and b are divisors of n, we see that n has a positive divisor not exceeding $\sqrt{n}$.
This divisor is either prime or, by the fundamental theorem of arithmetic, has a prime divisor less than itself. In either case, n has a prime divisor less than or equal to $\sqrt{n}$.

From Theorem 2, it follows that an integer is prime if it is not divisible by any prime less than or equal to its square root. This leads to the brute-force algorithm known as **trial division**. To use trial division we divide n by all primes not exceeding $\sqrt{n}$ and conclude that n is prime if it is not divisible by any of these primes.

THEOREM 3 There are infinitely many primes.

Proof: We will prove this theorem using a proof by contradiction. We assume that there are only finitely many primes, $p_1, p_2, \ldots, p_n$.

Let $Q = p_1 p_2 \cdots p_n + 1$.
By the fundamental theorem of arithmetic, Q is prime or else it can be written as the product of two or more primes.

However, none of the primes p_j divides Q, for if $p_j | Q$, then p_j divides $Q - p_1 p_2 \cdots p_n = 1$.

Hence, there is a prime not in the list $p_1, p_2, \ldots, p_n$.

This prime is either Q, if it is prime, or a prime factor of Q. This is a contradiction because we assumed that we have listed all the primes. Consequently, there are infinitely many primes.

Mersenne primes:

The largest prime known has been an integer of the special form $2^p - 1$, where p is also prime.

- Note that $2^n - 1$ cannot be prime when n is not prime;

Example: The numbers $2^2 - 1 = 3, 2^3 - 1 = 7, 2^5 - 1 = 31$ and $2^7 - 1 = 127$ are Mersenne primes, while $2^{11} - 1 = 2047$ is not a Mersenne prime because $2047 = 23 * 89$.

The largest Mersenne prime known (again as of early 2011) is $2^{43,112,609} - 1$, a number with nearly 13 million decimal digits, which was shown to be prime in 2008.

A communal effort, the Great Internet Mersenne Prime Search (GIMPS), is devoted to the search for new Mersenne primes.

THEOREM 4 THE PRIME NUMBER THEOREM

The ratio of the number of primes not exceeding x and $x/\ln x$ approaches 1 as x grows without bound. (Here $\ln x$ is the natural logarithm of x.)

The conjecture that every even integer n, $n > 2$, is the sum of two primes is now called **Goldbach's conjecture**. We can check this conjecture for small even numbers. For example, $4 = 2 + 2$, $6 = 3 + 3$, $8 = 5 + 3$, $10 = 7 + 3$, $12 = 7 + 5$, and so on.

Goldbach's conjecture was verified by hand calculations for numbers up to the millions prior to the advent of computers. With computers it can be checked for extremely large numbers. As of mid 2011, the conjecture has been checked for all positive even integers up to

$1.6 * 10^{18}$

- **The Twin Prime Conjecture Twin primes** are pairs of primes that differ by 2, such as 3 and 5, 5 and 7, 11 and 13, 17 and 19, and 4967 and 4969. The twin prime conjecture asserts that there are infinitely many twin primes

- The world's record for twin primes, as of mid 2011, consists of the numbers $65{,}516{,}468{,}355 * 2^{333{,}333} \pm 1$, which have $100{,}355$ decimal digits.

Greatest Common Divisors and Least Common Multiples

- **DEFINITION**
  Let a and b be integers, not both zero. The largest integer d such that $d|a$ and $d|b$ is called the *greatest common divisor* of a and b. The greatest common divisor of a and b is denoted by $\gcd(a, b)$.

Examples: What are the greatest common divisor of

(i) 17 and 22?

(ii) 24 and 36 ?

(iii) 37 and 237?

(iv) 251 and 29?

(v) 520 and 303?

DEFINITION

The integers a and b are *relatively prime* if their greatest common divisor (gcd) is 1.

Example:

The integers 17 and 22 are relatively prime, because $\gcd(17, 22) = 1$.

DEFINITION

The integers $a_1, a_2, \ldots, a_n$ are *pairwise relatively prime* if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

Example:

Determine whether the integers $10, 17$, and 21 are pairwise relatively prime and whether the integers $10, 19$, and 24 are pairwise relatively prime.

Another Approach to find gcd

- Another way to find the greatest common divisor of two positive integers is to use the prime factorizations of these integers. Suppose that the prime factorizations of the positive integers *a* and *b* are

$$a = p_1^{a_1} p_2^{a_2} \ldots . p_n^{a_n}, \quad b = p_1^{b_1} p_2^{b_2} \ldots . p_n^{b_n},$$

where each exponent is a nonnegative integer, and where all primes occurring in the prime factorization of either a or b are included in both factorizations, with zero exponents if necessary. Then $\gcd(a, b)$ is given by

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \ldots . p_n^{\min(a_n, b_n)}$$

where min*(x, y)* represents the minimum of the two numbers *x* and *y*.

Example: Find gcd of 120, 500 using prime factorization.

The prime factorizations of 120 and 500 are

$120 = 2^3 * 3 * 5$ and $500 = 2^2 * 5^3$, the greatest common divisor is

$$\gcd(120, 500) = 2^{\min(3,2)} 3^{\min(1,0)} 5^{\min(1,3)} = 2^2 3^0 5^1 = 20.$$

Least Common Multiples (lcm)

- The *least common multiple* of the positive integers a and b is the smallest positive integer that is divisible by both a and b. The least common multiple of a and b is denoted by $lcm(a, b)$.
- Suppose that the prime factorizations of the positive integers a and b are

$$a = p_1^{a_1} p_2^{a_2} \ldots . p_n^{a_n}, \; b = p_1^{b_1} p_2^{b_2} \ldots . p_n^{b_n},$$

where each exponent is a nonnegative integer, and where all primes occurring in the prime factorization of either a or b are included in both factorizations, with zero exponents if necessary. Then the least common multiple (lcm) of a and b is given by

$$lcm(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \ldots . p_n^{\max(a_n, b_n)}$$

where $\max(x, y)$ denotes the maximum of the two numbers x and y.

Example: What is the least common multiple of $2^3 3^5 7^2$ and $2^4 3^3$?

THEOREM 5

Let a and b be positive integers.

Then $ab = \gcd(a, b) \cdot lcm(a, b)$.

The Euclidean Algorithm

- A more efficient method of finding the greatest common divisor, called the **Euclidean algorithm**.
- This algorithm has been known since ancient times. It is named after the ancient Greek mathematician Euclid, who included a description of this algorithm in his book *The Elements*.

Lemma 1 Let $a = bq + r$, where a, b, q, and r are integers.

Then $\gcd(a, b) = \gcd(b, r)$.

Proof: If we can show that the common divisors of a and b are the same as the common divisors of b and r, implies that $\gcd(a, b) = \gcd(b, r)$, because both pairs must have the same *greatest* common divisor.

So suppose that d divides both a and b.

Then it follows that d also divides $a - bq = r$ (from Theorem 1 of Section1).

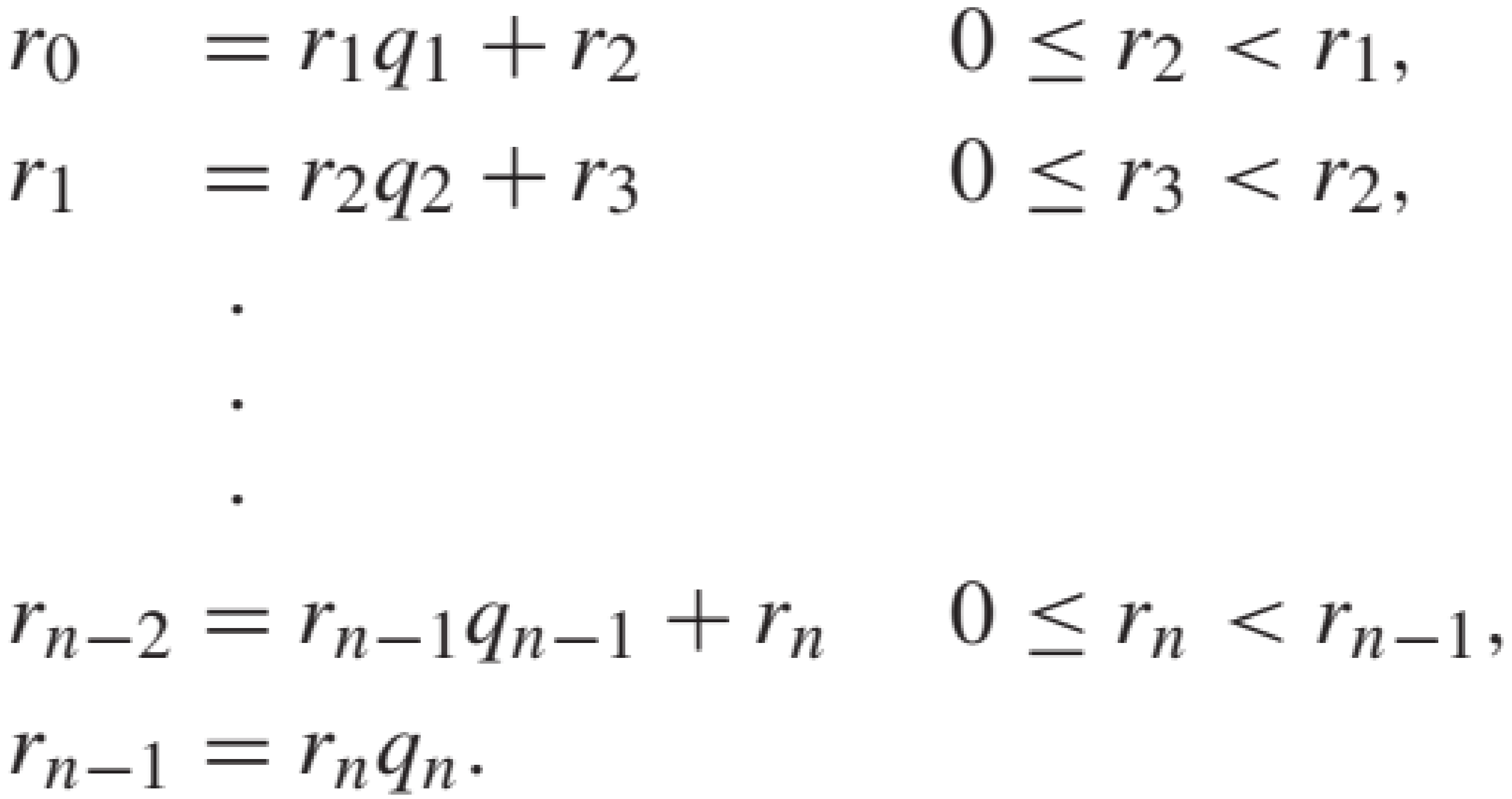
Hence, any common divisor of a and b is also a common divisor of b and r.

Likewise, suppose that d divides both b and r. Then d also divides $bq + r = a$.

Hence, any common divisor of b and r is also a common divisor of a and b.

Consequently, $\gcd(a, b) = \gcd(b, r)$.

Suppose that *a* and *b* are positive integers with $a \geq b$. Let $r_0 = a$ and $r_1 = b$. When we successively apply the division algorithm, we obtain



$$\begin{array}{lll}
r_0 & = r_1 q_1 + r_2 & 0 \leq r_2 < r_1, \\
r_1 & = r_2 q_2 + r_3 & 0 \leq r_3 < r_2, \\
 & \cdot & \\
 & \cdot & \\
 & \cdot & \\
r_{n-2} & = r_{n-1} q_{n-1} + r_n & 0 \leq r_n < r_{n-1}, \\
r_{n-1} & = r_n q_n . &
\end{array}$$

Eventually a remainder of zero occurs in this sequence of successive divisions, because the sequence of remainders $a = r_0 > r_1 > r_2 > \cdots \geq 0$ cannot contain more than a terms. Furthermore, it follows from Lemma 1 that

$$\begin{aligned}\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-2}, r_{n-1})\\ = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n.\end{aligned}$$

Hence, the greatest common divisor is the last nonzero remainder in the sequence of divisions.

EXAMPLE

Find the greatest common divisor of 414 and 662 using the Euclidean algorithm.

Solution: Successive uses of the division algorithm give:

$$
\begin{aligned}
662 &= 414 \cdot 1 + 248\\
414 &= 248 \cdot 1 + 166\\
248 &= 166 \cdot 1 + 82\\
166 &= 82 \cdot 2 + 2\\
82 &= 2 \cdot 41.
\end{aligned}
$$

Hence, $\gcd(414, 662) = 2$, because 2 is the last nonzero remainder.

gcds as Linear Combinations

- An important result we will use throughout the remainder of this Section is that the greatest common divisor of two integers a and b can be expressed in the form

$$sa + tb,$$

where s and t are integers.

In other words, $\gcd(a, b)$ can be expressed as a **linear combination** with integer coefficients of a and b.

For example, $\gcd(6, 14) = 2$, and $2 = (-2) \cdot 6 + 1 \cdot 14$.

The following Theorem (6) state the same fact.

BÉZOUT’S THEOREM

THEOREM 6 (BÉZOUT’S THEOREM)

If a and b are positive integers, then there exist integers s and t such that $\gcd(a, b) = sa + tb$.

Definition:

If a and b are positive integers, then integers s and t such that $\gcd(a, b) = sa + tb$ are called *Bézout coefficients* of a and b (after Étienne Bézout, a French mathematician of the eighteenth century).

Also, the equation $\gcd(a, b) = sa + tb$ is called *Bézout’s identity*.

Express gcd(252, 198) = 18 as a linear combination of 252 and 198.

Solution: To show that gcd(252, 198) = 18, the Euclidean algorithm uses these divisions:

$$\begin{aligned} 252 &= 1 \cdot 198 + 54 \\ 198 &= 3 \cdot 54 + 36 \\ 54 &= 1 \cdot 36 + 18 \\ 36 &= 2 \cdot 18. \end{aligned}$$

Using the next-to-last division (the third division), we can express gcd(252, 198) = 18 as a linear combination of 54 and 36. We find that

$$18 = 54 - 1 \cdot 36.$$

The second division tells us that

$$36 = 198 - 3 \cdot 54.$$

Substituting this expression for 36 into the previous equation, we can express 18 as a linear combination of 54 and 198. We have

$$18 = 54 - 1 \cdot 36 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198.$$

The first division tells us that

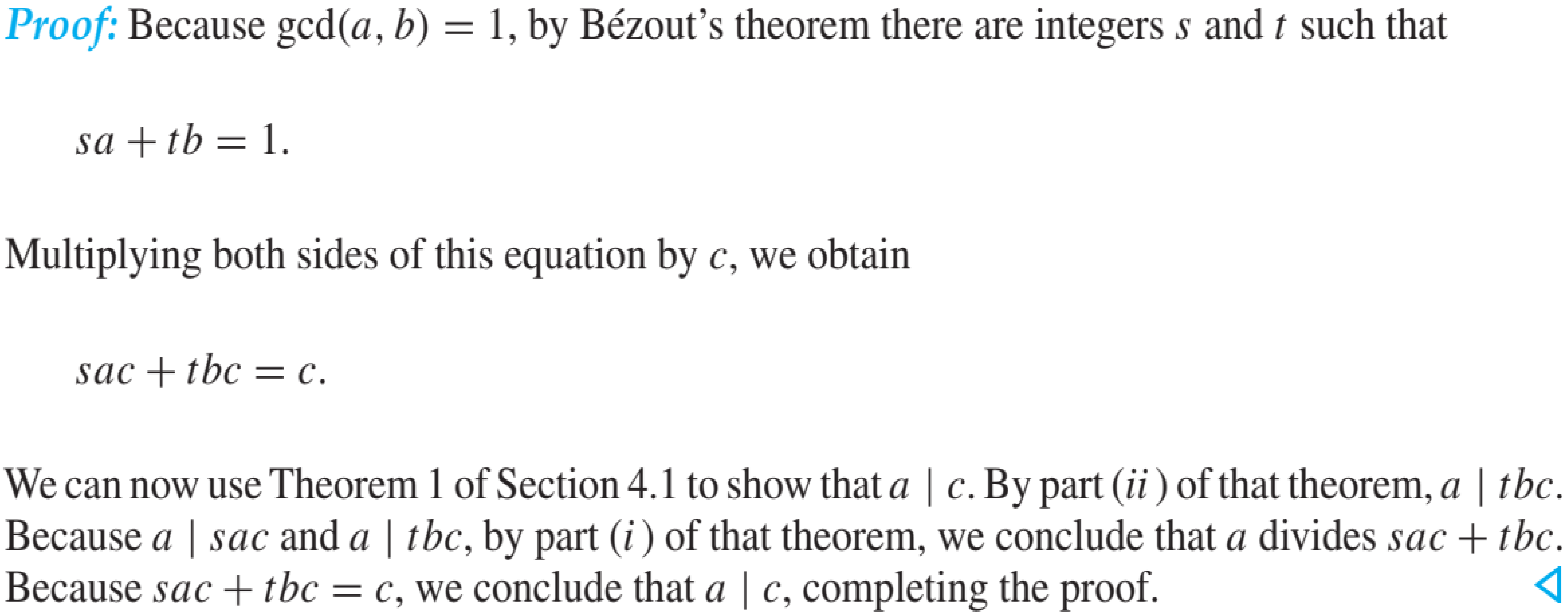
$$54 = 252 - 1 \cdot 198.$$

Substituting this expression for 54 into the previous equation, we can express 18 as a linear combination of 252 and 198. We conclude that

$$18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198,$$

LEMMA 2

If a, b, and c are positive integers such that $\gcd(a, b) = 1$ and $a | bc$, then $a | c$.



Proof: Because $\gcd(a, b) = 1$, by Bézout's theorem there are integers s and t such that

$$sa + tb = 1.$$

Multiplying both sides of this equation by c, we obtain

$$sac + tbc = c.$$

We can now use Theorem 1 of Section 4.1 to show that $a \mid c$. By part (ii) of that theorem, $a \mid tbc$. Because $a \mid sac$ and $a \mid tbc$, by part (i) of that theorem, we conclude that a divides $sac + tbc$. Because $sac + tbc = c$, we conclude that $a \mid c$, completing the proof. ◁

LEMMA 3 If p is a prime and $p \mid a_1a_2\cdots a_n$, where each a_i is an integer, then $p \mid a_i$ for some i.

THEOREM 7 Let m be a positive integer and let a, b, and c be integers. If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.

Proof: Because $ac \equiv bc \pmod{m}$, $m \mid ac - bc = c(a - b)$. By Lemma 2, because $\gcd(c, m) = 1$, it follows that $m \mid a - b$. We conclude that $a \equiv b \pmod{m}$. ◁