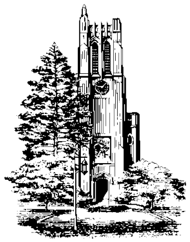
Divisibility and Modular Arithmetic

Sections 4.1& 4.3



Notables

- Homework due now!
- Reading Chapter 4
- Forthcoming topics
  - Integers and division
  - Integer representation and bases

Division

- If a and b are integers with $a \neq 0$, then *a divides b* if there exists an integer c such that $b = ac$.
- When a divides b we say
  - a is a *factor* of b
  - a is a *divisor* of b
  - b is a *multiple* of a.
- The notation $a \mid b$ denotes "a divides b".
  - $a \mid b$ if and only if b/a is an integer.
- The notation $a \nmid b$ denotes "a does not divide b"

Division

- **Exercise**: Which of the following are true?
  - $3 \mid 7$
  - $3 \mid 12$
  - $5 \nmid 15$

Properties of Divisibility

- **Theorem 1**: Let a, b, and c be integers, where $a \neq 0$.
  i. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;
  ii. If $a \mid b$, then $a \mid (bc)$ for all integers c;
  iii. If $a \mid b$ and $b \mid c$, then $a \mid c$.

If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$

- **Proof:**

  Suppose $a \mid b$ and $a \mid c$.

  Then there are integers s and t such that $b = as$ and $c = at$.

  Hence, $b + c = as + at = a(s + t)$.

  Since $(s + t)$ is an integer, it follows that $a \mid (b + c)$.

  Hence, if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.

  (ii), (iii) : Exercise (the proofs are similar to the proof above).

Properties of Divisibility

Theorem 1: Let a, b, and c be integers, where $a \neq 0$.

i. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;
ii. If $a \mid b$, then $a \mid (bc)$ for all integers c;
iii. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Corollary: If a, b, and c be integers such that $a \neq 0$ and $a \mid b$ and $a \mid c$, then $a \mid (mb + nc)$ whenever m and n are integers.

Exercise: Show how this Corollary follows from Theorem 1.

Properties of Divisibility

- **Lemma**: If n is a positive integer and a is a positive factor of n, then $1 \leq a \leq n$.
- Proof:

  Assume n is a positive integer and a is a positive factor of n.

  Then $n = ab$, for some integer b.

  Moreover, b must be positive since both n and a are.

  Hence $b \geq 1$.

  Multiplying by a we get: $n = ab \geq a \cdot 1 = a$.

  Thus, $1 \leq a \leq n$.

Division Algorithm

- **Division Algorithm (Theorem)**: If a is an integer and d is a positive integer, then there are unique integers q and r, with $0 \le r < d$, such that $a = dq + r$.
  - d is called the *divisor*.
  - a is called the *dividend*.
  - q is called the *quotient*.
  - r is called the *remainder*.

Definitions of **div** and **mod:**

$q = a$ **div** d
$r = a$ **mod** d

What other notation do we have for a **div** d?

$\lfloor a/d \rfloor$

Exercise

- Find the following:
  - 39 **div** 15 and 39 **mod** 15
  - 45 **div** 15 and 45 **mod** 15
  - -20 **div** 15 and -20 **mod** 15

Congruence Relation

- Definition: If a, b, and m are integers and $m > 0$, then *a is congruent to b modulo m* iff $m \mid (a - b)$.
  - $a \equiv b \pmod{m}$ stands for "a is congruent to b modulo m."
  - $a \not\equiv b \pmod{m}$ stands for "a is not congruent to b modulo m."
- Theorem: Two integers are congruent mod m if and only if they have the same remainder when divided by m. Proof: exercise

Exercise

- Which of the following are true?
  - $17 \equiv 5 \pmod{6}$
  - $24 \equiv 14 \pmod{6}$
  - $24 \equiv -14 \pmod{6}$
  - $-15 \equiv -15 \pmod{6}$

Exercise

- **Theorem 4**: Let m be a positive integer and a and b be integers. Then $a \equiv b \pmod{m}$ if and only if there is an integer k such that $a = b + km$.

Exercise

- **Theorem 4**: Let m be a positive integer and a and b be integers. Then $a \equiv b \pmod{m}$ if and only if there is an integer k such that $a = b + km$.
- Proof (more concisely):

Notation Hazard: ≡ (mod m) v.s. **mod**

- The "mod" in $a \equiv b \pmod{m}$ and a **mod** m are different.
  - $a \equiv b \pmod{m}$ is true iff $m \mid (a - b)$ is true.
  - a **mod** m denotes the remainder of a divided by m
    - Here, **mod** denotes a binary operation (function).

Relationship between ≡ (mod m) & **mod**

- **Theorem 3**: Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if (a **mod** m) = (b **mod** m). (Proof in the exercises)

Congruences of Sums and Products

- Theorem 5: Let m be a positive integer.
  If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then
  - $a + c \equiv b + d \pmod{m}$
  - $ac \equiv bd \pmod{m}$.
- Proof:
  Assume $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.
  Then, by Theorem 4, there are integers s and t such that $b = a + sm$ and $d = c + tm$.
  Therefore,
  $b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$ and
  $bd = (a + sm)(c + tm) = ac + m(at + cs + stm)$.
  Hence, by Theorem 4, $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

Congruences of Sums and Products

- Theorem 5: Let m be a positive integer.
  If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then
  - $a + c \equiv b + d \pmod{m}$
  - $ac \equiv bd \pmod{m}$.
- Example: Because $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$, it follows that $18 = 3 \pmod{5}$ and $77 = 2 \pmod{5}$.

Algebraic Manipulation of Congruences

- Multiplying both sides of a valid congruence by an integer preserves validity.

  I.e., if $a \equiv b \pmod{m}$, then $c \cdot a \equiv c \cdot b \pmod{m}$, where c is any integer.

  Proof: Theorem 5 since $c = c \pmod{m}$.

Algebraic Manipulation of Congruences

- Adding an integer to both sides of a valid congruence preserves validity.

  I.e., if $a \equiv b \pmod{m}$, then $c + a \equiv c + b \pmod{m}$, where c is any integer.

  Proof: Theorem 5 since $c = c \pmod{m}$.

Computing **mod** for Products and Sums

- Corollary: Let m be a positive integer and let a and b be integers. Then the following are true:
  - $(a + b)$ **mod** $m =$ $((a$ **mod** $m) + (b$ **mod** $m))$ **mod** m
  - ab **mod** $m = ((a$ **mod** $m)$ $(b$ **mod** $m))$ **mod** m.
- Exercise: Use this corollary to find the following
  - 240025 **mod** 12
  - ((39)(53)) **mod** 11

Arithmetic Modulo m

- Definitions: Let $\boldsymbol{Z}_m$ be the set of nonnegative integers less than m: $\boldsymbol{Z}_m = \{0,1, \ldots, m - 1\}$
- The operation $+_m$ is defined as $a +_m b = (a + b)$ **mod** m. This is *addition modulo m*.
- The operation $\cdot_m$ is defined as $a \cdot_m b = (a + b)$ **mod** m. This is *multiplication modulo m*.
- Using these operations is called *doing arithmetic modulo m*.
- Example: Find $7 +_{11} 9$ and $7 \cdot_{11} 9$.
- Solution: Using the definitions above:
  - $7 +_{11} 9 = (7 + 9)$ **mod** $11 = 16$ **mod** $11 = 5$
  - $7 \cdot_{11} 9 = (7 \cdot 9)$ **mod** $11 = 63$ **mod** $11 = 8$

Arithmetic Modulo m

- The operations $+_m$ and $\cdot_m$ satisfy many of the same properties as ordinary addition and multiplication.
  - Closure: If a and b belong to $\boldsymbol{Z}_m$, then $a +_m b$ and $a \cdot_m b$ belong to $\boldsymbol{Z}_m$.
  - Associativity: If a, b, and c belong to $\boldsymbol{Z}_m$, then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$.
  - Commutativity: If a and b belong to $\boldsymbol{Z}_m$, then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$.
  - Identity elements: If a belongs to $\boldsymbol{Z}_m$, then $a +_m 0 = a$ and $a \cdot_m 1 = a$.

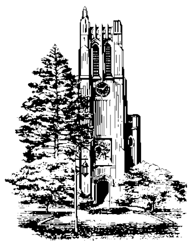
continued →

Arithmetic Modulo m

- *Additive inverses*: If $a \neq 0$ belongs to $\mathbf{Z}_m$, then $m - a$ is the additive inverse of a modulo m and 0 is its own additive inverse.
  - $a +_m (m - a) = 0$ and $0 +_m 0 = 0$
- *Distributivity*: If a, b, and c belong to $\mathbf{Z}_m$, then
  - $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ and $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$.
- Proofs are exercises.
- Multiplicative inverses have not been included since they do not always exist. For example, there is no multiplicative inverse of 2 modulo 6.
- (*optional*) Using the terminology of abstract algebra, $\mathbf{Z}_m$ with $+_m$ is a commutative group and $\mathbf{Z}_m$ with $+_m$ and $\cdot_m$ is a commutative ring.

Primes and Greatest Common Divisors

Sections 4.3



Primes

- **Definition:** A positive integer p greater than 1 is *prime* if the only positive factors of p are 1 and p.
- A positive integer that is greater than 1 and is not prime is called *composite*.

The Fundamental Theorem of Arithmetic

- **Prime FactorizationTheorem**:
  Every integer n greater than 1 can be written as the product of one or more primes—called the prime factorization of n.

  Additionally, the prime factorization of n is unique up to the order of the factors.

The Fundamental Theorem of Arithmetic

- Examples:
  - $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$
  - $641 = 641$
  - $999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$
  - $1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$

The Sieve of Erastosthenes

Erastothenes
(276-194 B.C.)

- A method for finding all primes that do not exceed a given positive integer, *n*.
  - List all of the integers from 2 to *n* in increasing order.

2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32

33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61

62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90

The Sieve of Erastosthenes

Erastothenes
(276-194 B.C.)

- A method for finding all primes that do not exceed a given positive integer, *n*.
  - List all of the integers from 2 to *n* in increasing order.
  - Mark the first unmarked element of the list as “prime”.

2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32

33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61

62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90

The Sieve of Erastosthenes

Erastothenes
(276-194 B.C.)

- A method for finding all primes that do not exceed a given positive integer, *n*.
  - List all of the integers from 2 to *n* in increasing order.
  - Mark the first unmarked element of the list as “prime”.
  - Delete all the unmarked integers that are divisible by the last element that was marked as “prime”.
  - Repeat the previous two steps until only marked integers are left.

2 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31

33 35 37 39 41 43 45 47 49 51 53 55 57 59 61

63 65 67 69 71 73 75 77 79 81 83 85 87 89

The Sieve of Erastosthenes

Erastothenes
(276-194 B.C.)

- A method for finding all primes that do not exceed a given positive integer, *n*.
  - List all of the integers from 2 to *n* in increasing order.
  - Mark the first unmarked element of the list as “prime”.
  - Delete all the unmarked integers that are divisible by the last element that was marked as “prime”.
  - Repeat the previous two steps until only marked integers are left.

2 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31

33 35 37 39 41 43 45 47 49 51 53 55 57 59 61

63 65 67 69 71 73 75 77 79 81 83 85 87 89

The Sieve of Erastosthenes

Erastothenes
(276-194 B.C.)

- A method for finding all primes that do not exceed a given positive integer, n.
  - List all of the integers from 2 to n in increasing order.
  - Mark the first unmarked element of the list as “prime”.
  - Delete all the unmarked integers that are divisible by the last element that was marked as “prime”.
  - Repeat the previous two steps until only marked integers are left.

2 3 5 7 11 13 17 19 23 25 29 31

35 37 41 43 47 49 53 55 59 61

65 67 71 73 77 79 83 85 89

The Sieve of Erastosthenes

Erastothenes
(276-194 B.C.)

- A method for finding all primes that do not exceed a given positive integer, n.
  - List all of the integers from 2 to n in increasing order.
  - Mark the first unmarked element of the list as “prime”.
  - Delete all the unmarked integers that are divisible by the last element that was marked as “prime”.
  - Repeat the previous two steps until only marked integers are left.

2 3 5 7 11 13 17 19 23 25 29 31

35 37 41 43 47 49 53 55 59 61

65 67 71 73 77 79 83 85 89

The Sieve of Erastosthenes

Erastothenes
(276-194 B.C.)

- A method for finding all primes that do not exceed a given positive integer, n.
  - List all of the integers from 2 to n in increasing order.
  - Mark the first unmarked element of the list as “prime”.
  - Delete all the unmarked integers that are divisible by the last element that was marked as “prime”.
  - Repeat the previous two steps until only marked integers are left.

2 3 5 7 11 13 17 19 23 29 31

37 41 43 47 49 53 59 61

67 71 73 77 79 83 89

The Sieve of Erastosthenes

Erastothenes
(276-194 B.C.)

- A method for finding all primes that do not exceed a given positive integer, n.
  - List all of the integers from 2 to n in increasing order.
  - Mark the first unmarked element of the list as “prime”.
  - Delete all the unmarked integers that are divisible by the last element that was marked as “prime”.
  - Repeat the previous two steps until only marked integers are left.

2 3 5 7 11 13 17 19 23 29 31

37 41 43 47 49 53 59 61

67 71 73 77 79 83 89

The Sieve of Erastosthenes

Erastothenes
(276-194 B.C.)

- A method for finding all primes that do not exceed a given positive integer, *n*.
  - List all of the integers from 2 to *n* in increasing order.
  - Mark the first unmarked element of the list as "prime".
  - Delete all the unmarked integers that are divisible by the last element that was marked as "prime".
  - Repeat the previous two steps until only marked integers are left.

2 3 5 7 11 13 17 19 23 29 31

37 41 43 47 53 59 61

67 71 73 79 83 89

The Sieve of Erastosthenes

Erastothenes
(276-194 B.C.)

- A method for finding all primes that do not exceed a given positive integer, *n*.
  - List all of the integers from 2 to *n* in increasing order.
  - Mark the first unmarked element of the list as "prime".
  - Delete all the unmarked integers that are divisible by the last element that was marked as "prime".
  - Repeat the previous two steps until only marked integers are left.

2 3 5 7 11 13 17 19 23 29 31

37 41 43 47 53 59 61

67 71 73 79 83 89

The Sieve of Erastosthenes

Erastothenes
(276-194 B.C.)

- A method for finding all primes that do not exceed a given positive integer, *n*.
  - List all of the integers from 2 to *n* in increasing order.
  - Mark the first unmarked element of the list as "prime".
  - Delete all the unmarked integers that are divisible by the last element that was marked as "prime".
  - Repeat the previous two steps until only marked integers are left.

2 3 5 7 11 13 17 19 23 29 31

37 41 43 47 53 59 61

67 71 73 79 83 89

And so on, until …

The Sieve of Erastosthenes

Erastothenes
(276-194 B.C.)

- A method for finding all primes that do not exceed a given positive integer, *n*.
  - List all of the integers from 2 to *n* in increasing order.
  - Mark the first unmarked element of the list as "prime".
  - Delete all the unmarked integers that are divisible by the last element that was marked as "prime".
  - Repeat the previous two steps until only marked integers are left.

2 3 5 7 11 13 17 19 23 29 31

37 41 43 47 53 59 61

67 71 73 79 83 89

The Sieve of Erastosthenes

Erastothenes
(276-194 B.C.)

- When could you stop marking numbers and just say "the remaining unmarked integers are all prime"?

The Sieve of Erastosthenes

Erastothenes
(276-194 B.C.)

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

  Proof: Assume n is composite.

  Then $n = ab$, for some integers, a and b, both greater than 1.

  We show by contradiction that either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

  Assume $a > \sqrt{n}$ and $b > \sqrt{n}$. (*)

  Then $ab > n$, which contradicts the choice of a and b.

  Hence, the assumption (*) must be false. QED.

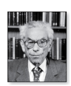
- This theorem justifies stopping at $\lfloor \sqrt{n} \rfloor$

Infinitude of Primes

Euclid
(325 B.C. – 265 B.C.)

- Theorem: There are infinitely many primes. (Euclid)
- Proof:
  - Assume that there are only n primes: $p_1, p_2, \ldots, p_n$
  - Let $q = p_1 p_2 \cdots p_n + 1$
  - Either q is prime or it is a product of primes (Fund. Thm. Arith.).
  - But none of the primes p_j divides q since if $p_j \mid q$, then p_j divides $q - p_1 p_2 \cdots p_n = 1$ and 1 has no prime factors.
  - As these are the only primes, q must be prime.
  - But $q > p_j$, for all the p_j.
  - So, contrary to our starting assumption, there are at least $n + 1$ primes.
  - Consequently, there are infinitely many primes.

This proof was given by Euclid *The Elements*. The proof is considered to be one of the most beautiful in all mathematics. It is the first proof in *The Book*, inspired by the famous mathematician Paul Erdős' imagined collection of perfect proofs maintained by God.



Paul Erdős
(1913-1996)

Generating Primes

- Finding large primes with hundreds of digits is important in cryptography.
- So far, no one has found a closed formula that always produces primes.
- $f(n) = n^2 - n + 41$ is prime for all integers $1,2,\ldots, 40$. But $f(41) = 41^2$ is not prime.
- More generally, there is no polynomial with integer coefficients such that $f(n)$ is prime for all positive integers n.
- Fortunately, we can generate large integers which are almost certainly prime.

Conjectures about Primes

Many conjectures about primes are unresolved, including:

- *Goldbach's Conjecture*: Every even integer n, $n > 2$, is the sum of two primes. This conjecture has been verified by computer for all positive even integers up to 1.6×10^{18}. It is believed to be true by most mathematicians.
- *The Twin Prime Conjecture*: The twin prime conjecture is that there are infinitely many pairs of twin primes. Twin primes are pairs of primes that differ by 2. Examples are 3 and 5, 5 and 7, 11 and 13, etc. The current world's record for twin primes (as of mid 2011) consists of numbers $65{,}516{,}468{,}355 \cdot 2^{333{,}333} \pm 1$, which have 100,355 decimal digits.

Greatest Common Divisor

- **Definition**: Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and also $d \mid b$ is called the *greatest common divisor* of a and b. It is denoted by gcd(a,b).
- Example: gcd(24, 36) = ?
- Example: gcd(17, 22) = ?
- Example: gcd(10024, 0) = ?

Finding gcd using prime factorizations

- Suppose the prime factorizations of a and b are:

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

where each exponent is a nonnegative integer, and where all primes occurring in either prime factorization are included in both. Then:

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

Finding gcd using prime factorizations

- Example: Find gcd(120, 500)
  - $120 = 2^3 \cdot 3 \cdot 5$
  - $500 = 2^2 \cdot 5^3$
    $= 2^2 \cdot 3^0 \cdot 5^3$
  - So, $\gcd(120, 500) = 2^2 \cdot 3^0 \cdot 5^1 = 20$

Finding gcd using prime factorizations

- Example: Find gcd(17, 22)
  - $17 = 17^1$
    $= 2^0 \cdot 11^0 \cdot 17^1$
  - $22 = 2^1 \cdot 11^1$
    $= 2^1 \cdot 11^1 \cdot 17^0$
  - So, gcd(17, 22) = $2^0 \cdot 11^0 \cdot 17^0 = 1$

Greatest Common Divisor

- **Definition**: The integers a and b are *relatively prime* if their greatest common divisor is 1.
  - Example: 17 and 22
- **Definition**: The integers $a_1, a_2, \ldots, a_n$ are *pairwise relatively prime* if gcd(a_i, a_j)= 1 whenever $1 \leq i < j \leq n$.

Greatest Common Divisor

- Exercise: Which of the following are pairwise relatively prime?
  - 10, 17 and 21
  - 10, 19 and 24
  - 25, 26, 9 and 121

Euclidean Algorithm

Euclid
(325 B.C. – 265 B.C.)

- The Euclidian algorithm is an efficient method for computing the greatest common divisor of two integers.
- It is based on the fact that, if $a > b$, then gcd(a, b) = gcd(b, a **mod** b).
- Example: Find gcd(91, 287):
  - 287 **mod** 91 = 14, so gcd(91, 287) = gcd(91, 14)
  - 91 **mod** 14 = 7, so gcd(91, 14) = gcd(14, 7)
  - 14 **mod** 7 = 0, so gcd(14, 7) = gcd(7, 0)
  - gcd(7, 0) = 7
  - Hence, gcd(91, 287) = 7

Euclidean Algorithm

Euclid
(325 B.C. – 265 B.C.)

- An efficient method for computing gcd.
- It is based on the fact that, if $a > b$, then $\gcd(a, b) = \gcd(b, a \textbf{ mod } b)$.
- Example: Find gcd(91, 287):
  - 287 **mod** 91 = 14, so gcd(91, 287) = gcd(91, 14)
  - 91 **mod** 14 = 7, so gcd(91, 14) = gcd(14, 7)
  - 14 **mod** 7 = 0, so gcd(14, 7) = gcd(7, 0)
  - gcd(7, 0) = 7
  - Hence, gcd(91, 287) = 7

Least Common Multiple

- **Definition**: The *least common multiple* of the positive integers a and b is the smallest positive integer that is divisible by both a and b. It is denoted by $\operatorname{lcm}(a,b)$.

Least Common Multiple

- If the prime factorizations of a and b are:
  $$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}\ , \quad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}\ ,$$
  where each exponent is a nonnegative integer, and where all primes occurring in either prime factorization are included in both. Then:
  $$\operatorname{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}$$

Least Common Multiple

- **Theorem 5**: Let a and b be positive integers. Then
  $$ab = \gcd(a,b) \cdot \operatorname{lcm}(a,b)$$
  Proof: Exercise.