NUMBER THEORY

YUCHENG JI

1. Divisor

A divisor of an integer n, also called a factor of n, is an integer which evenly divides n without leaving a remainder.

Example 1.1. 7 is a divisor of 35 because $35/7 = 5$. We also say 35 is divisible by 7, or 35 is a multiple of 7, or seven divides 35 and we usually write $7 \mid 35$.

In general, we say $m \mid n$ (read: m divides n) for non-zero integers, if there exists an integer k such that $n = km$. Thus divisors can be negative as well as positive e.g. divisors of 6 are 1, 2, 3, 6, -1, -2, -3, -6 but one would usually mention the positive ones 1, 2, 3, 6.

1 and -1 divide (are divisors of) every integer, every integer is a divisor of itself and every integer is a divisor of 0. A divisor of n that is not 1,-1, n or n is known as non-trivial divisor, numbers with non-trivial divisors are known as composite numbers while prime numbers have non-trivial divisors.

If $a \mid b = c$, then a is the dividend, b the divisor and c the quotient.

A *prime* number has exactly two divisors, 1 and itself.

Question 1.2. Is 1 a prime number?

Question 1.3. Compute the number of divisors of 23, 24, 25, and 26.

Question 1.4. The divisors of a number come in pairs. Does that mean that every number has an even number of divisors?

Question 1.5. Is there a number with exactly 9 divisors?

Date: November 13th, 2016.

Question 1.6. Special Question: The Locker Problem

A row of lockers is numbered 1 through 100 down the hallway. The 1st math circle student celebrates the beginning of the school year by running down the hallway, opening each locker.

The 2nd math circle student runs down the hallway and closes every 2nd locker $2, 4, 6, 8, ...$

The 3rd math circle student runs down the hallway and changes every third locker $3, 6, 9, 12, ...$ from open to shut or shut to open, depending on its position at the time.

This celebration continues. After the 100th student runs down the hallway and changes the position of the 100th locker, which lockers will be open?

2. Least Common Multiple (LCM)

Definition 2.1. *The least common multiple of p and q is defined as the smallest positive integer that is divisible by both p and q. It may be denoted as $[p, q]$.*

Example 2.2. Examples:

$$[4, 9] = 36$$
$$[-3, 4] = 12$$
$$[7, 8] = 56$$

Calculation of LCM using prime factors:

Example 2.3. Find the LCM of 16, 24 and 840.
Step 1:Express each of the numbers as prime factors

$$16 = 2^4$$
$$24 = 23 \times 3$$
$$840 = 23 \times 3 \times 5 \times 7$$

Step 2: Pick out the highest power of each of the prime factors that appears. The factors need not be common. For example, the highest powers of 2, 3, 5 and 7 are 4, 1, 1, and the LCD becomes $24 \times 3 \times 5 \times 7 = 1680$.

Question 2.4. Find the LCMS of

$$18, 20, 24;$$
$$30, 45, 50;$$
$$252, 990, 3150;$$
$$450, 2100, 990.$$

3. Greatest Common Divisor (GCD)

Definition 3.1. *Any two integers p and q have at least one positive divisor in common, called greatest common divisor (gcd).*

If at least one of the integers p and q is different from zero, then there exists a largest positive integer d which divides both p and q.

This integer dis called the greatest common divisor (gcd) of p and q and may be denoted as gcd (p, q) or (p, q).

Example 3.2. Examples:

$$(6, 12) = 3$$
$$(0, 18) = (0, -18) = 18$$
$$(9, 27) = 9$$

Calculation of GCD using prime factors:

Example 3.3. Find the GCD of 60, 100, and 840. Step 1:Express each of the numbers as prime factors

$$60 = 2^3 \times 3 \times 5$$
$$100 = 2^2 \times 5^2$$
$$840 = 23 \times 3 \times 5 \times 7$$

Step 2: Pick out the highest common power of each common factor. The product of these highest powers gives the GCD. For example, the common prime factors are 2 and 5. The highest powers of 2 and 5 which are common are $2^2 \times 5 = 20$ their GCD.

Question 3.4. Find the GCDS of

$$540, 72, 378;$$
$$30, 45, 50;$$
$$105, 546, 231;$$
$$1125, 675.$$

4. Eulidean Algorithm

Eulidean algorithm (Euclid's algorithm) is an algorithm to determine the greatest common divisor (GCD) of two integers by repeatedly dividing the two numbers and the remainder in turns.

Description of the algorithm:

Given two natural numbers m and n, check if $n = 0$. If yes, m is the gcd. If not, repeat the process using n and the remainder after integer division of m and n.

Theorem 4.1. *Either m is a multiple of n, or there is a positive integer k, and integers q_1,q_2,...,q_k, r_1, r_2,...,r_{k-1} (and $r_k = 0$) such that*

$$\begin{aligned}
&m = q_1 \times n + r_1 (0 \leq r_1 < n)\\
&n = q_2 \times r_1 + r_2 (0 \leq r_1 < r_2)\\
&...\\
&...\\
&r_{k-3} = q_{k-1} \times r_{k-2} + r_{k-1} (0 \leq r_{k-1} < r_{k-2})\\
&r_{k-2} = q_k \times r_{k-1} (r_k = 0).
\end{aligned}$$

r_{k-1} is the GCD of m and n.

Example 4.2. Find the GCD of 5775 and 1008. Solution:

$$m = 5775, n = 1008.$$

$$\begin{gathered}
5775 = 5 \times 1008 + 735\\
1008 = 1 \times 735 + 273\\
735 = 2 \times 273 + 189\\
189 = 2 \times 84 + 21\\
84 = 4 \times 21
\end{gathered}$$

Thus the GCD= 21 is the largest integer that divides 5775 and 1008.

Question 4.3. Find the GCDS of

$$\begin{gathered}
1021, 1079;\\
2261, 1275.
\end{gathered}$$

Using the Eulidean algorithm.

Question 4.4. Find the GCD of $x^2 - 4x + 1$ and $5x$.

Question 4.5. Special Question:
The numbers in the sequence 101, 104, 109, 116,...are of the form $a_n = 100+n^2$, where $n = 1, 2, 3, ...$ For each n, let d_n be the greatest common divisor of a_n and $a_n + 1$. Find the maximum value of d_n as n ranges through the positive integers.

Question 4.6. Special Question:
What is the largest positive integer n such that $n^3 + 100$ is divisible by $n + 10$?

E-mail address: yuchenj@uci.edu

Rowland Hall, University of California, Irvine, CA 92697