Training Handout Numbers

$a \mid b$: a is a factor of b, (i.e. b is divisible by a.)
GCF: Greatest Common Factor (also known as Greatest Common Divisor – **GCD**.)
Notation: $\gcf(a, b)$, $\gcf(a, b, c)$, etc.
LCM: Least Common Multiple.
Notation: $\text{lcm}(a, b)$, $\text{lcm}(a, b, c)$, etc.

- If a_1 and a_2 are natural numbers and if dividing a_1 by a_2 yields q as the quotient and a_3 as the remainder, i.e. $a_1 = q \cdot a_2 + a_3$, with $0 \le a_3 < a_2$, then the set of common factors of a_1 and a_2 equals the set of common factors of a_2 and a_3. It follows that $\gcf(a_1, a_2) = \gcf(a_2, a_3)$.
  This simple observation leads to many important facts laid out below.
- **The Euclidean Algorithm** for finding the greatest common: Apply the fact above repeatedly by carrying out a sequence of long divisions until the remainder vanishes, as illustrated below.
  Example: $\gcf(1071, 1029) = \gcf(1029, 42) = \gcf(42, 21) = 21$ after carrying out a sequence of long divisions:
  $$1071 = 1 \times 1029 + 42$$
  $$1029 = 24 \times 42 + 21$$
  $$42 = 2 \times 21 + 0$$
- Representing GCF as $\gcf(a, b) = sa + tb$: $\gcf(a, b)$ can always be written in the form $sa + tb$, where $s, t \in Z$. Namely, **the GCF of a and b can be expressed as a linear combination of a and b with integer coefficients.** (The choice of coefficients s and t is not unique.) This can be generalized to cases involving the GCF of three or more natural numbers.
  The proof follows from unwinding the steps in the Euclidean Algorithm, as illustrated by the following example.
  Example: $\gcf(1071, 1029) = 21 = -24 \times 1071 + 25 \times 1029$ by unwinding the long divisions shown above: The second from last line gives $21 = 1029 - 24 \times 42$. Then use the line before (the first line) to express 42 as $1071 - 1 \times 1029$ and substitute this for 42 to get
  $21 = 1029 - 24 \times 42 = 1029 - 24 \times (1071 - 1 \times 1029) = -24 \times 1071 + 25 \times 1029$.
- **Important Fact:** If p is a <u>prime</u>, and $p \mid (ab)$, then either $p \mid a$ or $p \mid b$. (The assertion is not true if p is not a prime!!!!)
  Proof: Suppose p is not a factor of a, then we will have to show $p \mid b$. But p is a prime, so if p is not a factor of a we will have $\gcf(p, a) = 1$, thus $1 = sp + ta$ for some $s, t \in Z$. Multiply both sides by b to get $b = spb + tab$. But $p \mid ab$, so $p \mid tab$, thus it is clear from this expression for b that $p \mid b$.

*This immediately gives the well known "***Unique Prime Factorization***":*

- Every natural number has a <u>unique</u> prime factorization. And $a \mid b$ precisely when the prime factorization of a is part of that of b.

With this picture in mind, we now easily see:

- A number is a common factor of several natural numbers if and only if it is a factor of their GCF.
- A number is a common multiple of several natural numbers if and only if it is a multiple of their LCM.

The following facts are very useful:

- The GCF of a and b equals the GCF of a and the difference of a and b.
- $\gcf(a, b) \cdot \text{lcm}(a, b) = ab$

Modular Arithmetic

- Let n be a natural number
  For $a, b \in Z$, we say a and b are "congruent modulo n" if the difference $a - b$ is divisible by n. We write "$a \equiv b \pmod{n}$".
  When working with Z modulo n, we "overlook" anything that's a multiple of n.
  Example: Working with Z modulo 3, we have really only three elements: $-1, 0, 1$. For instance, 3, 6, -3, -6 are considered the same as 0, and 2, 5, -4, -7 are considered the same as -1.
- Good news: The congruence relation modulo n is compatible with $+$ and $\times$:
  If $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$, then
  (1) $a_1 b_1 \equiv a_2 b_2 \pmod{n}$
  (2) $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$
  (3) $-a_1 \equiv -a_2 \pmod{n}$
  (4) $a_1 - b_1 \equiv a_2 - b_2 \pmod{n}$
  (5) $a_1^{\,k} \equiv a_2^{\,k} \pmod{n}$ for any $k = 1, 2, 3, \cdots$
  This means that, working modulo n, you can do the usual addition and multiplication, and you are free to change any integer to another that is congruent to it, modulo n, at any stage.
  Example: $2^{13} + 7^9 \equiv (-1)^{13} + (1)^9 = -1 + 1 = 0 \pmod 3$.
  So $2^{13} + 7^9 \equiv 0 \pmod 3$, which simply means that $2^{13} + 7^9$ is divisible by 3.
- If we work modulo p, with p a prime, then another piece of good news is that we can even make sense out of reciprocal and division! For example, working modulo 7, each number not congruent to 0 has a reciprocal: The reciprocal of 2 is 4 (which is the same as, say, -3, 11, 18) and the reciprocal of 3 is -2 (which is the same as, say, -9, 5, 12.)
  Proof: Suppose a is not 0 (modulo p). This means a is not divisible by p.
  But p is a prime, it follows that $\gcf(a, p) = 1$, and so there are $s, t \in Z$ such that $sa + tp = 1$. Thus $sa \equiv 1 \pmod{p}$, and so r is the reciprocal of a.
  Note: It is essential that p is a prime.

Divisibility Rules

The machinery and language of modular arithmetic allows for simple proofs of many divisibility rules.

- Divisibility by 3: A natural number is divisible by 3 if and only if the sum of its digits is divisible by 3. If fact, the natural number is congruent (mod 3) to the sum of its digits.
  E.g., 126981 is divisible by 3 as the digits sum to 27, which is divisible by 3.
  Proof: Say we have a four-digit natural number a with digits d_3, d_2, d_1, d_0 from left to right. Then
  $a = d_3 \cdot 10^3 + d_2 \cdot 10^2 + d_1 \cdot 10^1 + d_0 \equiv d_3 \cdot 1^3 + d_2 \cdot 1^2 + d_1 \cdot 1^1 + d_0 = d_3 + d_2 + d_1 + d_0$ (mod 3).
- Divisibility by 9: A natural number is divisible by 9 if and only if the sum of its digits is divisible by 9. In fact, the natural number is congruent (mod 9) to the sum of its digits. (The proof is similar to that for divisibility by 3.)
- Divisibility by 11: A natural number is divisible by 11 if and only if the **alternating sum** of its digits is divisible by 11. In fact, the natural number is congruent (mod 11) to the alternating sum of its digits (with the ones digit given positive sign in the sum.)
  Example: 91438061 is divisible by 11 because $1-6+0-8+3-4+1-9=-22$ is divisible by 11.
  Proof: Follow the same idea as in the proof of divisibility by 3, and use the fact that $10 \equiv -1$ (mod 11).
- Divisibility by 7: If d is the ones digit of the natural number a, and c is the what is left when the ones digit d is erased, then a is divisible by 7 if and only if $c-2d$ is divisible by 7. (Unfortunately, it is NOT true that a is congruent to $c-2d$ modulo 7 when a is not divisible by 7! E.g., Although 101 is not divisible by 7 because $10-2\cdot 1=8$ is not divisible by 7, it is however not true that 101 is congruent to 8 modulo 7. From the proof below, we see that it is $3(c-2d)$, not $c-2d$, that is always congruent to a modulo 7.)
  Example: To decide if 2009 is divisible by 7, we have to see if $200-2\cdot 9=182$ is divisible by 7. For this, again, we have to see if $18-2\cdot 2=14$ is divisible by 7. But this is obviously true, so 2009 is divisible by 7.
  Proof: $a = 10c + d \equiv 3c + d \equiv 3c - 6d = 3(c-2d)$ (mod 7). Thus a is divisible by 7 if and only if $3(c-2d)$ is divisible by 7. But $3(c-2d)$ is divisible by 7 if and only if $c-2d$ is divisible by 7.