Set 2

(A) Warm-up problems:

(1) Perform division with remainder for the following pairs (a, b): (103, 5), (47, 20), (85, 5), (40, 1).

(2) Recall: if a, d are integers, we say that d divides a (abbreviated $d|a$) if there is an integer k such that $a = kd$. Show that 3 divides 6, and that 5 does not divide 7.

(3) If a is a positive integer, the *divisors* of a are all the positive integers that divide a. For example, the divisors of 6 are $\{1, 2, 3, 6\}$ and the divisors of 4 are $\{1, 2, 4\}$. Write down the divisors of 8, the divisors of 9, and the divisors of 12.

(4) If a, b are two positive integers, the *common divisors* of a and b, denoted $\mathrm{CD}(a, b)$, are the positive integers that are divisors of a and b simultaneously. For example, the common divisors of 4 and 6 are $\mathrm{CD}(4, 6) = \{1, 2\}$. The list of common divisors is a finite list, and hence it has a biggest element, which is called the *greatest common divisor* of a and b and is denoted as $\gcd(a, b)$. For example, $\gcd(4, 6) = 2$. Find the list of common divisors of 8 and 12, and then find $\gcd(8, 12)$.

(5) If a, b are two positive integers, a *linear combination* of a and b is an integer c that can be written as $c = ax + by$ for some integers x, y. Show that 5 is a linear combination of 10 and 25.

One of the goals for today will be to prove the following.

Theorem 1. *Let a, b be positive integers. Then $\gcd(a, b)$ is the smallest positive integer g that can be written as $g = ax + by$ for some integers x and y. That is, $\gcd(a, b)$ is the smallest positive linear combination of a and b.*

(B)

(1) Verify that the theorem is true for these values of (a, b): $(3, 5)$, $(3, 6)$, $(6, 15)$.

(2) (***HW***) Verify that the theorem is true for $(a, b) = (6, 10)$.

(3) Perform the Euclidean algorithm for the following values of (a, b): $(108, 51)$, $(98, 47)$, $(32, 14)$, $(125, 45)$. In each case, show that the last remainder is $\gcd(a, b)$.

(4) For the pairs (a, b) of the previous problem, use "backwards substitution" on the Euclidean algorithm to find integers x and y so that $\gcd(a, b) = ax + by$. Convince yourself that, whenever the last remainder of the Euclidean algorithm for (a, b) is $\gcd(a, b)$, then we can find integers x and y for which $\gcd(a, b) = ax + by$. In the next problem, we will show that the last remainder of the Euclidean algorithm is always $\gcd(a, b)$.

(5) Suppose we perform the Euclidean algorithm on two positive integers a and b. Let us call $a = r_0$ and $b = r_1$. We obtain a list of equations:

$$\begin{aligned}
r_0 &= q_1 r_1 + r_2 && (0 \le r_2 < r_1) \\
r_1 &= q_2 r_2 + r_3 && (0 \le r_3 < r_2) \\
r_2 &= q_3 r_3 + r_4 && (0 \le r_4 < r_3) \\
&\vdots \\
r_n &= q_n r_{n+1} + 0 && (0 \le r_{n+1} < r_n)
\end{aligned}$$

Why is it that the Euclidean algorithm must always terminate (that is: why do we always get to a step where the remainder is zero)?

(6) Show that

$$\mathrm{CD}(r_0, r_1) = \mathrm{CD}(r_1, r_2) = \cdots = \mathrm{CD}(r_n, r_{n+1}),$$

and use this to conclude that $r_n = \gcd(a, b)$. Explain why this proves Theorem 1.

(7) Notice that the Euclidean algorithm for $(a, b) = (108, 51)$ took 3 steps, and that for $(a, b) = (32, 14)$ or $(a, b) = (125, 45)$ it took 4 steps. Can you cook up (a, b) so that the Euclidean algorithm for (a, b) takes 5 steps?

(8) Perform the Euclidean algorithm for $(a, b) = (34, 21)$. If you are familiar with the Fibonacci numbers, you may notice a pattern.

(9) (***HW***) Explain why the gcd of any two consecutive Fibonacci numbers is 1.

(C)

(1) This chain of exercises gives a "non-constructive" proof of Theorem 1. It is called "non-constructive" because, unlike the proof that uses the Euclidean algorithm, this proof does not tell you how to find x and y.

  (i) Let h denote the smallest positive element in the set $X = \{ax + by \mid x, y \in \mathbb{Z}\}$, and let $g = \gcd(a, b)$. Show that g divides h, and therefore $g \leq h$.

  (ii) Show that h divides a. [Hint: If h does not divide a, use the division algorithm to write $a = qh + r$ with $0 \leq r < h$, and show that r is in the set X. This is a contradiction, since h was the smallest positive element of X]. Similarly, show that h divides b.

  (iii) Finish the proof.

(2) Let a, b be positive integers. Show that an integer n can be written as $ax + by$ for $x, y \in \mathbb{Z}$ if and only if n is a multiple of $\gcd(a, b)$. In set-theoretic notation, this statement is written as:

$$\{\alpha x + \beta y \mid x, y \in \mathbb{Z}\} = \mathbb{Z} \cdot \gcd(a, b).$$

(3) (***HW***) Suppose that a number a has exactly 3 divisors. Show that a must be the square of a prime number.

(D) Suppose we have a circle with $n(= 1, 2, 3, ...)$ points labeled on its circumference, and we draw all the possible chords connecting those n points to one another. Assuming that no three chords intersect in a common point (which we can always assume by moving the points slightly), count the number of regions into which the chords divide the circle. Do you notice a pattern? Again ask yourself: when will you have assembled enough evidence to be convinced of any pattern you detect, and how would you justify it beyond any doubt?

(E) We typically represent integers in base 10, i.e. when we write 1014 we mean $1 \cdot 10^3 + 0 \cdot 10^2 + 1 \cdot 10^1 + 4 \cdot 10^0$. We could just as well use different bsaes, for instance base 7. The integer 1014 (a base 10 expression) can be expressed in base 7 as $2 \cdot 7^3 + 6 \cdot 7^2 + 4 \cdot 7^1 + 6 \cdot 7^0$ (check this!); let us write $1014 = (2646)_7$ to indicate this base 7 expression.

(1) Express the (given in base 10) integers 97 and 512 in base 7.

(2) Compute the following sums and products in base 7, without first converting to base 10: $(365)_7 + (104)_7$; $(25)_7 \cdot (6)_7$; $(142)_7 \cdot (15)_7$.

(3) If an integer's base 7 expression $(a_n a_{n-1} \ldots a_0)_7$ is given to you (that is, the integer $a_n 7^n + a_{n-1} 7^{n-1} + \cdots + a_0 7^0$), find a simple divisibility test (in terms of the base 7 "digits" $a_n, \ldots, a_0$) for whether the integer is divisible by 7. Also find tests for divisibility by 6 and by 8.