HOMEWORK #1 SOLUTIONS

Remember to write clearly and to justify all your claims in your solutions.

(1) Use induction to prove that

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}. \tag{1}$$

Solution. First, we prove the base case of the above formula, when $n = 1$. This is obvious, since then the formula reads $1^2 = 1(2)(3)/6 = 1$, which is true.

Next, we assume that the formula is true for n, and prove it true for $n+1$. The formula for n reads

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}.$$

Add $(n+1)^2$ to both sides:

$$\left(\sum_{k=1}^{n} k^2\right) + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2.$$

The left hand side is the same as the sum of the squares from 1 to $n+1$. The right hand side simplifies to:

$$\begin{aligned} \frac{n(n+1)(2n+1) + 6(n+1)^2}{6} &= \frac{(n+1)(n(2n+1) + 6(n+1))}{6} \\ = \frac{(n+1)(2n^2 + 7n + 6)}{6} &= \frac{(n+1)(n+2)(2n+3)}{6} \end{aligned}$$

This last expression is the same as the right hand side of Equation 1, with n replaced by $n+1$. So we have proven Equation 1 with n replaced by $n+1$, which was our goal. □

(2) Use the Euclidean algorithm to find the gcd of the following pairs of integers:
(a) $a = 186, b = 51$,
(b) $a = 438, b = 150$.
You should write down each step of the Euclidean algorithm (although you need not show all your arithmetic scratchwork).

Solution. For $a = 186, b = 51$, we get the following list of Euclidean divisions:

$$\begin{aligned}186 &= 51 \cdot 3 + 33 (q = 3, r = 33),\\ 51 &= 33 \cdot 1 + 18 (q = 1, r = 18),\\ 33 &= 18 \cdot 1 + 15 (q = 1, r = 15),\\ 18 &= 15 \cdot 1 + 3 (q = 1, r = 3),\\ 15 &= 3 \cdot 5 + 0 (q = 5, r = 0).\end{aligned}$$

The last non-zero remainder, 3, is the gcd of 186 and 51. □

For $a = 438, b = 150$, we get the following list of Euclidean divisions:

$$\begin{aligned}438 &= 150 \cdot 2 + 138 (q = 2, r = 138),\\ 150 &= 138 \cdot 1 + 12 (q = 1, r = 12),\\ 138 &= 12 \cdot 11 + 6 (q = 11, r = 6),\\ 12 &= 6 \cdot 2 + 0 (q = 2, r = 0).\end{aligned}$$

The last non-zero remainder, 6, is the gcd of 438 and 150. □

(3) Use the Euclidean algorithm to find a pair of integer solutions x, y to the equation $96x + 28y = 8$. (Soon we will see how to find all integer solutions to this equation.)

Solution. We begin by using the Euclidean algorithm to find the gcd of 96 and 28:

$$\begin{aligned}96 &= 28 \cdot 3 + 12,\\ 28 &= 12 \cdot 2 + 4,\\ 12 &= 4 \cdot 3 + 0.\end{aligned}$$

The last non-zero remainder is 4, so $\gcd(96, 28) = 4$. We now use the steps of the Euclidean algorithm to find a pair of integers x, y which solve the equation $96x + 28y = 4$:

$$\begin{aligned}4 &= 28 - 12(2),\\ 4 &= 28 - (96 - 28 \cdot 3)(2) = 96(-2) + 28(7).\end{aligned}$$

Therefore $x = -2, y = 7$ solves $96x+28y = 4$. To get a solution to $96x+28y = 8$, just multiply the previous solutions by 2, so that $x = -4, y = 14$ solves $96x + 28y = 8$. □

(4) Suppose we know that the gcd of two positive integers, say a, b, is equal to 20. Is it possible to determine what all the (positive) common divisors of a, b are from this information? If so, what are those common divisors? (Remember, you need to prove all your assertions!)

Solution. A theorem in class said that every common divisor of a, b divides $\gcd(a, b) = 20$ as well. Just to be thorough, we should check that every divisor of $\gcd(a, b)$ is also a common divisor of a, b. So suppose $c | \gcd(a, b)$. Because $\gcd(a, b)|a, b$, we must have $c|a, c|b$, as desired.

These two facts taken together show that the set of common divisors of a, b are just the divisors of $\gcd(a, b) = 20$. The divisors of 20 are $1, 2, 4, 5, 10, 20$, so these are the common divisors of a, b. $\square$

(5) Recall that the *Fibonacci sequence* f_n is defined by the recursive relation $f_{n+2} = f_{n+1} + f_n$ for $n \geq 1$, and the initial terms $f_1 = f_2 = 1$. So the first few members of the Fibonacci sequence are $1, 1, 2, 3, 5, 8, \ldots$. Show that $\gcd(f_{n+1}, f_n) = 1$ for all $n \geq 1$.

Solution. If we want to prove something about $\gcd(f_{n+1}, f_n)$, it might be worthwhile to try the Euclidean algorithm. So let $n \geq 3$ be any integer greater than 2. (If $n = 1, 2$, then the claim in the question is obviously true.) Let us try a Euclidean division of f_{n+1} by f_n. The recursive definition of the Fibonacci sequence tells us that $f_{n-1} = f_{n+1} - f_n$. Also notice that $f_{n-1} < f_n$: indeed, since $f_n > 0$ for all n, and $f_{n-1} + f_{n-2} = f_n$, we must have $f_{n-1} < f_n$ since $f_{n-2} > 0$. Therefore, f_{n-1} must be the remainder when we perform a Euclidean division of f_{n+1} by f_n. (Remember, the remainder is the unique integer r such that $0 \leq r < f_n$, and such that $f_{n+1} - r$ is a multiple of f_n.)

But if f_{n-1} is the remainder when we perform a Euclidean division of f_{n+1} by f_n, this tells us that $\gcd(f_{n+1}, f_n) = \gcd(f_n, f_{n-1})$. We repeat this argument with f_n, f_{n-1} to obtain the following chain of equalities:

$$\gcd(f_{n+1}, f_n) = \gcd(f_n, f_{n-1}) = \ldots = \gcd(f_3, f_2) = \gcd(2, 1) = 1. \ \square$$

(6) For each of the following sets of integers, determine whether they are mutually coprime, not mutually coprime but coprime, or not coprime. (Remember, prove your answer.)
(a) $27, 80, 13$,
(b) $24, 19, 186$.

Solution. The set $27, 80, 13$ is mutually coprime. Indeed, $27 = 3^3$, and $3 \nmid 80$, so $\gcd(27, 80) = 1$. Since 13 is prime, and $13 \nmid 27, 80$, $\gcd(13, 27) = 1, \gcd(13, 80) = 1$.

The set $24, 19, 186$ is coprime but not mutually coprime. For instance, $3|24, 3|186$, so $\gcd(24, 186) \geq 3$. However, because 19 is prime, and $19 \nmid 24$, $\gcd(24, 19, 186) = \gcd(\gcd(24, 19), 186) = \gcd(1, 186) = 1$. $\square$

(7) For a positive integer n, let $\phi(n)$ be the number of positive integers less than n coprime to n. For instance, $\phi(4) = 2$, since $1, 3$ are coprime to 4, but 2 is not, while $\phi(6) = 2$ as well, because $1, 5$ are coprime to 6, but $2, 3, 4$ are not. (This function is called the *Euler totient* function and we will learn much more about it later in the class.)
(a) Calculate $\phi(3)$ and $\phi(12)$.
(b) Calculate $\phi(5)$ and $\phi(15)$. What is the relationship between $\phi(5), \phi(3)$, and $\phi(15)$?
(c) Based on the above calculations, if a, b are positive integers, what do you conjecture for the relationship between $\phi(a), \phi(b)$, and $\phi(ab)$? (Don't bother trying to prove your conjecture, we'll do this later on.)
(d) Test your conjecture with $a = 4, b = 2$. Do you need to change your conjecture at all? (Presumably you will need to calculate $\phi(2)$ and $\phi(8)$.)

Solution.

(a) $\phi(3) = 2$, since $\gcd(1,3) = \gcd(2,3) = 1$, while $\gcd(3,3) = 3 \neq 1$. Similarly, $\phi(12) = 4$, because $\gcd(1,12) = \gcd(5,12) = \gcd(7,12) = \gcd(11,12) = 1$, while $\gcd(n,12) \neq 1$ for any other value of $n, 1 \leq n \leq 12$ (those other values are divisible by either 2 or 3).

(b) $\phi(5) = 4$, because 5 is prime, so that $\gcd(n,5) = 1$ for $1 \leq n < 5$. $\phi(15) = 8$, since $1,2,4,7,8,11,13,14$ are relatively prime to 15 (they are not divisible by either 3 or 5), while $3,5,6,9,10,12,15$ are not relatively prime to 15.

(c) The above considerations seem to suggest that $\phi(ab) = \phi(a)\phi(b)$.

(d) If $a = 4, b = 2$, we have $\phi(2) = 1, \phi(4) = 2, \phi(8) = 4$, so the conjecture from the previous part fails for this choice of a, b. The correct modification is to require that a, b be relatively prime in our conjecture, which is the case with the a, b pairs $3, 4$ or $5, 3$. $\square$