Fall 2021 – Math 328K – 55385

Midterm exam with solutions

Thursday, October 7, 14:00

Problem 1. Define the terms "greatest common divisor" and "coprime".

Solution 1. The *greatest common divisor* (a, b) of integers a, b, not both 0, is the greatest positive integer $d \in \mathbb{Z}_+$ such that $d \mid a$ and $d \mid b$. The greatest common divisor $(0, 0)$ of 0 and itself is 0.

Two integers a, b are *coprime* if $(a, b) = 1$.

Problem 2. Let a and b be positive integers. Show that

$$\gcd(a, b) \cdot \operatorname{lcm}(a, b) = a \cdot b,$$

where $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ are the greatest common divisor and the least common multiple of a and b.

Solution 2. By the Fundamental Theorem of Number Theory, a and b can be written as products of prime powers

$$a = p_1^{i_1} \cdots p_n^{i_n} \qquad b = p_1^{j_1} \cdots p_n^{j_n},$$

where $p_1, \ldots, p_n$ are distinct primes and $i_1, \ldots, i_n, j_1, \ldots, j_n \geq 0$. We proved in class that then

$$\gcd(a, b) = p_1^{\min\{i_1, j_1\}} \cdots p_n^{\min\{i_n, j_n\}}, \qquad \operatorname{lcm}(a, b) = p_1^{\max\{i_1, j_1\}} \cdots p_n^{\max\{i_n, j_n\}}.$$

Now consider every prime separately. We have

$$p_k^{\min\{i_k, j_k\}} \cdot p_k^{\max\{i_k, j_k\}} = p_k^{\min\{i_k, j_k\} + \max\{i_k, j_k\}} = p_k^{i_k + j_k} = p_k^{i_k} \cdot p_k^{j_k}$$

for every $k \in \{1, \ldots, n\}$. So $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = a \cdot b$.

Problem 3. The *Fibonnacci numbers* $f_1, f_2, f_3, \ldots$ are recursively defined by

$$f_1 = 1, \quad f_2 = 1, \quad f_{n+2} = f_{n+1} + f_n \ \forall n \in \mathbb{N}.$$

Show that $\sum_{i=1}^{n} f_i^2 = f_n f_{n+1}$ for every $n \in \mathbb{N}$.

Solution 3. We use induction over n, starting at $n = 1$. For the base step, we just verify that $\sum_{i=1}^{1} f_i^2 = f_1^2 = 1 = f_1 f_2$.

For the inductive step, assume that the equality $\sum_{i=1}^{n} f_i^2 = f_n f_{n+1}$ is known. We want to show $\sum_{i=1}^{n+1} f_i^2 = f_{n+1} f_{n+2}$. This follows from the computation

$$f_{n+1} f_{n+2} = f_{n+1}(f_n + f_{n+1}) = f_n f_{n+1} + f_{n+1}^2 = \sum_{i=1}^{n} f_i^2 + f_{n+1}^2 = \sum_{i=1}^{n+1} f_i^2,$$

where we used the induction hypothesis in the third step.

Problem 4. For which integers $c \in \mathbb{Z}$ does the equation

$$9x = c \bmod 75$$

have a solution $x \in \mathbb{Z}/75\mathbb{Z}$? In the cases which have solutions, find all of them.

Solution 4. Since $(9, 75) = 3$ the equation has a solution if and only if $3 \mid c$, and has 3 solutions in that case.

Assume that $3 \mid c$, then we can write $c = 3n$ for some integer n. Since

$$9 \cdot (-8) \bmod 75 = -72 \bmod 75 = 3 \bmod 75$$

$[-8n]$ is a solution of the equation. The other two solutions are $[25 - 8n]$ and $[50 - 8n]$.

Problem 5. Let $p > 3$ be a prime number. Show that

$$2^{p-2} + 3^{p-2} + 6^{p-2} \bmod p = 1 \bmod p.$$

Solution 5. Let $x = [2^{p-2} + 3^{p-2} + 6^{p-2}] \in \mathbb{Z}/p\mathbb{Z}$. Then

$$[6]x = [6]\cdot[2]^{p-2} + [6]\cdot[3]^{p-2} + [6]\cdot[6]^{p-2} = [3]\cdot[2]^{p-1} + [2]\cdot[2]^{p-1} + [6]^{p-1} = [3]+[2]+[1] = [6],$$

using Fermat's little theorem in the third step. Since p and 6 are coprime, $[6]$ is invertible. So $x = [1]$.