

Final Exam Solutions

Problem #1a: Suppose that apples cost 15 cents each, while oranges cost 40 cents each. Mary has a 5 dollar note and wants to spend it all on apples and oranges. If she wants the number of apples and oranges she buys to be as equal as possible, how many apples and oranges can she buy?

Proof: Let x be the number of apples that Mary buys and y be the number of oranges that she buys. We are looking for integer solutions to

$$15x + 40y = 500.$$

Since $GCF(15, 40) = 5$ and $5 \mid 500$, we know that there will be solutions. We will use the Euclidean algorithm:

$$40 = 15(2) + 10$$

$$15 = 10(1) + 5$$

$$10 = 5(2) + 0.$$

From this, we work backwards to get

$$\begin{aligned} 5 &= 15 - 10(1) \\ &= 15 - (40 - 15(2)) \\ &= 15(3) + 40(-1). \end{aligned}$$

Multiplying this equation through by 100 gives

$$15(300) + 40(-100) = 500.$$

So we have $x = 300$ and $y = -100$ as a solution to the equation. However, we are looking for x and y to be as close as possible (and we also want them positive), so we need a formula for the general solution:

$$\begin{aligned} x &= 300 - \frac{40}{5}t = 300 - 8t \\ y &= -100 + \frac{15}{5}t = -100 + 3t \end{aligned}$$

We now want to pick the value of t so that the difference $x - y$ is as small as possible:

$$x - y = (300 - 8t) - (-100 + 3t) = 400 - 11t.$$

The difference is 0 when $t = 400/11$, and the nearest integer to that is 36. So

$$\begin{aligned} x &= 300 - 8(36) = 12 \\ y &= -100 + 3(36) = 8 \end{aligned}$$

Comment: If you wanted, you could have divided out the 5 at the beginning and look for solutions to

$$3x + 8y = 100.$$

Problem #2a: Give Euclid's proof that there are infinitely prime numbers.

Proof: Suppose for a contradiction that there are only finitely many primes and call them p_1, p_2, \dots, p_r . Consider the number $N = p_1 p_2 \cdots p_r + 1$. We know that N is either prime or composite.

Suppose N is prime. Notice that $N \neq p_i$ for all i by definition. This means that N is a prime that isn't on the list of all primes, giving a contradiction.

Suppose N is composite. Then let q be a prime dividing N . We know that $q = p_i$ for some i since the p_i is a complete list of all primes. But since $q \mid (p_1 p_2 \cdots p_r)$ and $q \mid N$, we have

$$q \mid N - p_1 p_2 \cdots p_r = 1.$$

But no primes divide 1, and we have a contradiction.

In both situations, we get a contradiction, so the initial assumption must be false. Therefore, there are infinitely many primes.

Problem #2b: Let p_n be the n -th prime. Using (a) and mathematical induction, show that

$$p_n \leq 2^{2^{n-1}}.$$

Proof: We use the second principle of mathematical induction.

Suppose that the statement is true for $n < k$, that is,

$$p_i \leq 2^{2^{i-1}}$$

for $i = 1, 2, \dots, k-1$. We must show that

$$p_k \leq 2^{2^{k-1}}.$$

Let $N = p_1 p_2 \cdots p_{k-1} + 1$. We know that none of the p_i divide N (for otherwise, p_i would divide 1). Either N will be a prime or it will be a composite. In either case, p_k (the next prime) can be no larger than N . Therefore,

$$\begin{aligned} p_k &\leq N \\ &\leq p_1 p_2 \cdots p_{k-1} + 1 \\ &\leq 2^{2^0} \cdot 2^{2^1} \cdot 2^{2^2} \cdots 2^{2^{k-2}} + 1, \text{ by the inductive hypothesis} \\ &\leq 2^{1+2+4+\cdots+2^{k-2}} + 1 \\ &\leq 2^{2^{k-1}-1} + 1 \\ &\leq \left(\frac{1}{2}\right) 2^{2^{k-1}} + 1 \end{aligned}$$

Clearly, we have

$$1 \leq \left(\frac{1}{2}\right) 2^{2^{k-1}},$$

so we have

$$\begin{aligned} p_k &\leq \left(\frac{1}{2}\right) 2^{2^{k-1}} + \left(\frac{1}{2}\right) 2^{2^{k-1}} \\ &\leq 2^{2^{k-1}}. \end{aligned}$$

Problem #2c: Show that there are infinitely many primes of the form $3k + 2$.

Proof: Suppose there are only finitely many such primes and call them p_1, p_2, \dots, p_r . Consider the number $N = (p_1 p_2 \cdots p_r)^2 + 1$. Notice that $N \equiv 2 \pmod{3}$ since for each i , $p_i^2 \equiv 1 \pmod{3}$ so that the product is also 1 modulo 3.

Suppose N is prime. Notice that $N \neq p_i$ for all i by definition. This means that N is a prime that isn't on the list of all primes, giving a contradiction.

Suppose N is composite. Notice that all the primes q dividing N must be of the form $3k + 1$ since none of the p_i can divide N . But the product of numbers of the form $3k + 1$ is also of the form $3k + 1$, contradicting that N is of the form $3k + 2$.

Problem #3a: Let p be a prime and let a be an integer not divisible by p . What does it mean to say that a is a quadratic residue mod p ? Give the definition of the Legendre symbol.

Proof: We say that a is a quadratic residue mod p if there is a solution to $x^2 \equiv a \pmod{p}$. The Legendre symbol is defined for $GCD(a, p) = 1$ by

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{if } a \text{ is a quadratic residue mod } p \\ -1, & \text{if } a \text{ is not a quadratic residue mod } p. \end{cases}$$

Problem #3b: For which primes $p > 3$ does the quadratic congruence $x^2 \equiv 6 \pmod{p}$ have solutions?

Proof: We are looking for primes such that

$$\left(\frac{6}{p}\right) = +1.$$

Notice that

$$\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right) \left(\frac{3}{p}\right).$$

By quadratic reciprocity,

$$\left(\frac{3}{p}\right) \left(\frac{p}{3}\right) = (-1)^{\frac{(3-1)(p-1)}{4}} = (-1)^{\frac{p-1}{2}},$$

so that we have

$$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right).$$

Pulling these equations together, we want to find p so that

$$(-1)^{\frac{p-1}{2}} \left(\frac{2}{p}\right) \left(\frac{p}{3}\right) = +1.$$

For the first term, we have

$$(-1)^{\frac{p-1}{2}} = \begin{cases} +1, & \text{if } p \equiv 1 \pmod{4} \\ -1, & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

For the second term, we have

$$\left(\frac{2}{p}\right) = \begin{cases} +1, & \text{if } p \equiv 1, 7 \pmod{8} \\ -1, & \text{if } p \equiv 3, 5 \pmod{8}. \end{cases}$$

For the third term, we have

$$\left(\frac{p}{3}\right) = \begin{cases} +1, & \text{if } p \equiv 1 \pmod{3} \\ -1, & \text{if } p \equiv 2 \pmod{3}. \end{cases}$$

Notice that the moduli for the first two congruences are not relatively prime. Since $LCM(4, 8) = 8$, we will need to consider these two together mod 8 in each of the cases below.

There are four combinations that can make this product +1.

For the (+++) case, we have two situations to consider. The first is

$$\begin{aligned} p &\equiv 1 \pmod{4} \\ p &\equiv 1 \pmod{8} \\ p &\equiv 1 \pmod{3} \end{aligned}$$

The first two congruences are solved by $p \equiv 1 \pmod{8}$, so we need

$$\begin{aligned} p &\equiv 1 \pmod{8} \\ p &\equiv 1 \pmod{3} \end{aligned}$$

It is easy to see that this is equivalent to $p \equiv 1 \pmod{24}$. (This situation is small enough that you can do it in your head.) The second situation is

$$\begin{aligned} p &\equiv 1 \pmod{4} \\ p &\equiv 7 \pmod{8} \\ p &\equiv 1 \pmod{3} \end{aligned}$$

The first two congruences cannot be solved together, so there are no more possibilities from this situation.

I will condense the rest of the cases in the interest of space. The $(+--)$ case gives

$$\begin{aligned} p &\equiv 5 \pmod{8} \\ p &\equiv 2 \pmod{3} \end{aligned}$$

which is solved by $p \equiv 5 \pmod{24}$. The $(-+-)$ case gives

$$\begin{aligned} p &\equiv 3 \pmod{8} \\ p &\equiv 2 \pmod{3} \end{aligned}$$

which is solved by $p \equiv 11 \pmod{24}$. The $(--+)$ case gives

$$\begin{aligned} p &\equiv 3 \pmod{8} \\ p &\equiv 1 \pmod{3} \end{aligned}$$

which is solved by $p \equiv 19 \pmod{24}$.

Putting all the cases together, when $p \equiv 1, 5, 11, 19 \pmod{24}$, we have

$$\left(\frac{6}{p}\right) = +1$$

Problem #3c: Find all solutions to $x^2 - 6x + 14 \equiv 0 \pmod{149}$.

Proof: Notice that 149 is prime. We begin by completing the square.

$$\begin{aligned} x^2 - 6x + 14 &\equiv 0 \pmod{149} \\ (x^2 - 6x + 9) + 5 &\equiv 0 \pmod{149} \\ (x - 3)^2 &\equiv -5 \pmod{149} \\ (x - 3)^2 &\equiv 144 \pmod{149} \\ x - 3 &\equiv \pm 12 \pmod{149} \\ x &\equiv 3 \pm 12 \pmod{149} \\ x &\equiv -9, 15 \pmod{149} \end{aligned}$$

Problem #4: I'm not retyping the whole problem. It translates to finding a solution x with $900 \leq x \leq 1200$ to the following system of congruences:

$$\begin{aligned} x &\equiv 1 \pmod{10} \\ x &\equiv 2 \pmod{9} \\ x &\equiv 0 \pmod{7} \end{aligned}$$

Proof: From the first congruence, we know that $x = 1 + 10k_1$ for some integer k_1 . We plug this into the second congruence to get

$$1 + 10k_1 \equiv 2 \pmod{9} \implies k_1 \equiv 1 \pmod{9}.$$

So we have $k_1 = 1 + 9k_2$ for some integer k_2 . This implies that $x = 1 + 10(1 + 9k_2) = 11 + 90k_2$. Finally, we plug this into the third congruence to get

$$11 + 90k_2 \equiv 0 \pmod{7} \implies -k_2 \equiv -4 \pmod{7}.$$

So $k_2 = 4 + 7k_3$ for some integer k_3 . Then we have $x = 11 + 90(4 + 7k_3) = 371 + 630k_3$.

We need to pick k_3 so that x satisfies the inequalities. It is easy to see that $k_3 = 1$ works and that this gives $x = 1001$.

Problem #6a: If $GCD(a, b, c) = 1$, then a, b, c are pairwise relatively prime.

FALSE: We have $GCD(6, 15, 10) = 1$ but $GCD(6, 15) = 3$.

Problem #6b: If f and g are two multiplicative functions, then the function $f + g$, defined by $(f + g)(x) = f(x) + g(x)$ is also multiplicative.

FALSE: We know that ϕ and σ are multiplicative functions. But

$$(\phi + \sigma)(6) = \phi(6) + \sigma(6) = 2 + 12 = 14$$

while

$$(\phi + \sigma)(2) \cdot (\phi + \sigma)(3) = (1 + 3) \cdot (2 + 4) = 4 \cdot 6 = 24.$$

Problem #6d: There are no integer solutions to the equation $x^2 - 5y^2 = 17$.

TRUE: Consider this equation mod 5:

$$x^2 \equiv 2 \pmod{5}.$$

Since 1 and 4 are the only squares mod 5, we know that there are no solutions to the equation.

Problem #6e: If p is an odd prime, one can find integers x and y satisfying $x^2 + y^2 \equiv -1 \pmod{p}$.

TRUE: Notice that this is equivalent to solving

$$x^2 \equiv -(y^2 + 1) \pmod{p}.$$

Consider the values of $x^2 \pmod{p}$. We know that there are exactly $(p+1)/2$ values. Now consider the values of $-(y^2 + 1) \pmod{p}$. There are also exactly $(p+1)/2$ values of this. If we combine the two lists together, we have $p+1$ values (not necessarily distinct). Since there are only p possible values mod p , by the pigeon-hole principle, there must be a repeated value. Pick the x and y corresponding to this repeated value.

I have had fun being your TA this quarter. Good luck on your finals. – Aaron