Math 342 Tutorial

May 28, 2025

Question 1. Prove that if a and b are different integers, then there exist infinitely many positive integers n such that $a+n$ and $b+n$ are coprime. [Hint: Consider linear combinations of $b-a$ and $1-a$ if $a < b$.]

Assume that $a < b$, and let $n = (b-a)k + (1-a)$. We have that $n > 0$ for large enough k. Now $a + n = (b-a)k + 1$ and $b + n = (b-a)(k+1) + 1$, hence $a+n,\ b+n > 0$. If we had $d \mid a+n,\ b+n$, we would have $d \mid a-b$ and so $d \mid 1$ since $d \mid a+n$. Thus, $d = 1$ and $(a+n,\ b+n) = 1$.

Here is an additional solution pointed out by several in the class. Let p be a prime greater than b, and write $n = p - b > 0$. Since $a < b$, we have $a + n < b + n = p$. As p is prime, $(a+n,\ b+n) = 1$. Since there are infinitely many primes greater than b, there are infinitely many n satisfying the requirement. This solution is valid here because we only asked for infinitely many such n. If instead we were required to provide a closed form solution for each n, then we would need to provide something like the first solution.

Question 2. Prove that every integer > 6 can be represented as a sum of two integers > 1 which are coprime. [Hint. Consider the three cases $n = 4k \pm 1$, $n = 4k$, and $n = 4k + 2$ seperately, and write the summands interms of k].

The easy case is if $n > 6$ is odd, for then $n = 2 + (n-2)$ and clearly $(2,\ n-2) = 1$. Next, consider the case $n = 4k$. Then $n = (2k+1) + (2k-1)$ where certainly $(2k+1,\ 2k-1) = 1$ and $2k + 1 > 2k - 1 > 1$ as $k > 1$. Finally, consider the case $n = 4k + 2$. We have that $4k + 2 = (2k+3) + (2k-1)$. If $d \mid 2k+3,\ 2k-1$, then $d \mid (2k+3) - (2k-1) = 4$. Since d must be odd, we have that $d = 1$. Observe further that $2k + 3 > 2k - 1 > 1$ as $k > 1$.

Question 3. An integer n is *powerful* if, whenever a prime p divides n, p^2 divides n. Show that every powerful integer n can be written as the product of a perfect square and a perfect cube.

The exponents in the nonredundant prime power factorization of a are all at least 2. If a is a square, we're done as we can write $a = u^2 1^3$. Therefore, assume a is not a perfect square. Let $p_1, \ldots,\ p_k$ be the primes appearing with even exponent, and let $q_1, \ldots,\ q_l$ be the primes with odd exponent. Since the odd exponents are at least 3, we can write

$$a = p_1^{2e_1} \cdots p_k^{e_k} q_1^{2f_1+3} \cdots q_l^{2f_l+3} \quad \text{for } e_i,\ f_i \geqq 0.$$

But then

$$a = (p_1^{e_1} \cdots p_k^{e_k} q_1^{f_1} \cdots q_l^{f_l})^2 (q_1 \cdots q_l)^3$$

as required.

Question 4. Show that $(a,\ b) \mid [a,\ b]$. When does $(a,\ b) = [a,\ b]$?

We have $(a,\ b) \mid a$ and $a \mid [a,\ b]$, hence $(a,\ b) \mid [a,\ b]$. Let $a = p_1^{r_1} \cdots p_k^{r_k}$ and $b = p_1^{s_1} \cdots p_k^{s_k}$. Then $(a,\ b) = [a,\ b]$ if and only if $\min\{r_i,\ s_i\} = \max\{r_i,\ s_i\}$. If $r_i < s_i$, then $\max\{r_i,\ s_i\} = s_i \neq r_i = \min\{r_i,\ s_i\}$ which contradicts our assumption that $\max\{r_I,\ s_i\} = \min\{r_i,\ s_i\}$. Thus, $r_i \geqq s_i$. Similarly, however, $s_i < r_i$ cannot happen. We are left with $r_i = s_i$ which shows that $a = b$.

Question 5. Show that if $a, b, c > 0$, then

$$(a,\ b,\ c)[ab,\ ac,\ bc] = abc = (ab,\ ac,\ bc)[a,\ b,\ c].$$

Let $a\,b,\ c$ have prime factorizations $a = p_1^{r_1}\cdots p_k^{r_k}$, $b = p_1^{s_1}\cdots p_k^{s_k}$, $c = p_1^{t_1}\cdots p_k^{t_k}$. Then $p_i^{r_i+s_i+t_i}\|abc$, but $p_i^{\min\{r_i,s_i,t_i\}}\|(a,\ b,\ c)$ and $p_i^{r_i+s_i+t_i-\min\{r_i,s_i,t_i\}}\|[ab,\ ac,\ bc]$, and $p_i^{r_i+s_i+t_i-\min\{r_i,s_i,t_i\}}p_i^{\min\{r_i,s_i,t_i\}} = p^{r_i+s_i+t_i}$. Therefore, $(a,\ b,\ c)[ab,\ ac,\ bc] = abc$. One may similarly show that $[a,\ b,\ c](ab,\ ac,\ bc) = abc$.

Question 6. An arithmetic function $f : \mathbf{N} \to \mathbf{C}$ is *multiplicative* if $f(mn) = f(m)f(n)$ whenever $(m,\ n) = 1$. The summatory function F of an arithmetic function $f : \mathbf{N} \to \mathbf{C}$ is defined as $F(x) = \sum_{d|x} f(d)$. The number of divisors functions is defined as $\tau(x) = \#\{d : d \mid x\}$. **(a)** Show that every summatory function of a multiplicative function is multiplicative. **(b)** Show the number of divisors function is multiplicative. **(c)** If $n = p_1^{e_1}\cdots p_k^{e_k}$, show that $\tau(n) = (e_1+1)\cdots(e_k+1)$. **(d)** Prove that for every positive integer k, the set of all positive integers n whose number of positive integer divisors is divisible by k contains an infinite arithmetic progression. [Hint: Consider a progression defined by a linear combination of consecutive powers of 2, and use part (c).]

(a) Let $m, n > 0$ be such that $(m,\ n) = 1$. Thus, every divisor d of mn can be written as $d = d'd''$ where $d' \mid m$ and $d'' \mid n$ with $(d',\ d'') = 1$. Observe, therefore, that

$$F(mn) = \sum_{d|mn} f(d) = \sum_{\substack{d'|m \\ d''|n}} f(d'd'') = \sum_{\substack{d'|m \\ d''|n}} f(d')f(d'') = \sum_{d'|m} f(d') \sum_{d''|n} f(d'') = F(m)F(n).$$

We have shown that F is multiplicative.

(b) Let $id(x) = 1$ be the constant function which maps every integer x to 1. Certainly, id is multiplicative. Observe $\tau(a) = \sum_{d|x} id(x) = \sum_{d|x} 1 = \#\{d : d \mid x\}$. From part (a), we have that τ is therefore multiplicative.

(c) Consider the prime power p^e, $e \geqq 0$. The divisors of p^e are $1,\ p, \ldots,\ p^e$. So, p^e has $e+1$ divisors. Writing $n = p_1^{e_1}\cdots p_k^{e_k}$, and from part (b), we see that

$$\tau(n) = \tau(p_1^{e_1})\cdots\tau(p_k^{e_k}) = (e_1+1)\cdots(e_k+1).$$

(d) We consider the infinite progression $2^k n + 2^{k-1}$ for $n \geqq 0$. We can write the general term as $2^{k-1}(2n+1)$ where obviously $2^{k-1}\|2^{k-1}(2n+1)$. From parts (b) and (c) above, $\tau(2^k n + 2^{k-1}) = \tau(2^{k-1})\tau(2n+1) = k\tau(2n+1)$. We have, therefore, an infinite progression satisfying the required property.

Question 7. Prove that there exists infinitely many triplets of positive integers $x,\ y,\ z$ for which the numbers $x(x+1),\ y(y+1),\ z(z+1)$ form an increasing arithmetic progression. [Hint: write y and z as increasing linear functions of x.]

Let $x > 0$ be arbitrary, and define $y = 5x+2$ and $z = 7x+3$. Then

$$y(y+1) - x(x+1) = z(z+1) - y(y+1) = 24x^2 24x + +6 > 0 \quad \text{since } x > 0.$$

Question 8. Prove that for every even $n > 6$ there exist primes p and q such that $(n-p,\ n-q) = 1$.

It suffices to take $p = 3$ and $q = 5$. If $n > 6$ is even, the we have $n - 1 \geqq 6$ and $p < q < n-1$. The numbers $n - p = n - 3$ and $n - q = n - 5$ as consecutive odd numbers, are relatively prime.

Question 9. **(a)** Prove that for every three consecutive odd integers, one must be divisible by 3. [Hint. Write $n = 2k+1$ and consider the possible cases for k (mod 3).] **(b)** Find all primes which can be represented as both a sum and difference of primes.

(a) Let k be an arbitrary integer, and consider the consecutive integers $2k+1$, $2k+3$, and $2k+5$. If $k \equiv 0 \pmod 3$, then $2k+3 \equiv 0 \pmod 3$. If $k \equiv 1 \pmod 3$, then $2k+1 \equiv 0 \pmod 3$. If $k \equiv 2 \pmod 3$, then $2k+5 \equiv 0 \pmod 3$. In every case, we have that one of $2k+1$, $2k+3$, and $2k+5$ is divisible by 3. Since k was arbitrary, the result follows.

(b) Suppose that r is an arbitrary prime that can be represented simultaneously as a sum and difference of two pairs of prime numbers. Certainly, $r \neq 2$, hence $r > 2$ must be odd. Therefore, one of the primes from each pair of representing primes must be even, i.e., we have that $r = p + 2 = q - 2$ for some odd primes p, q. But then p, r, q are three consecutive odd prime. From part (a), $(p,\ r,\ q) = (3,\ 5,\ 7)$ are the only three consecutive odd primes so that $r = 5$ is the only solution.

Question 10. Find all integer solutions x, y of the equation $2x^3 + xy - 7 = 0$ and prove that this equation has infinitely many solutions in positive rationals. [Hint: Use the possible values for x in the first part to infer a possible form for x in the second part.]

Since $x(2x^2 + y) = 7$, we have that $x = \pm 1,\ \pm 7$. Upon substituting these values for x, we find that $y = 5,\ -97,\ -9,\ -99$ as the possible values for y.

Let $n > 5$ be arbitrary, and let $x = 7/n$ so that $y = \frac{n-98}{n^2}$. These are rational and positive solutions to $2x^3 + xy - 7 = 0$.

Question 11. An astronomer knows that a satellite orbits the Earth in a period that is an exact multiple of 1 hour that is less than 1 day. If the astronomer notes that the satellite completes 11 orbits in an interval that starts when a 24-hour clock reads 0 hours and ends when the clock reads 17 hours, how long is the orbital period of the satellite?

This is equivalent to finding solutions to $11x \equiv 17 \pmod{24}$. By Theorem 4.11, there is a unique solution given by $x \equiv 19 \pmod{24}$. So the satellite orbits the Earth every 19 hours.

Question 12. **(a)** Let p be an odd prime. Show the congruence $x^2 \equiv 1 \pmod{p^k}$ has exactly two incongruent solutions, namely, $x \equiv \pm 1 \pmod{p^k}$. **(b)** Show that the congruence $x^2 \equiv 1 \pmod{2^k}$ has exactly four incongruent solutions, namely, $x \equiv \pm 1 \pm (1 - 2^{k-1}) \pmod{2^k}$, when $k > 2$. Show there is one when $k = 1$ and two when $k = 2$.

(a) If $x^2 \equiv 1 \pmod{p^k}$, then $x^2 - 1 = (x-1)(x+1) \equiv 0 \pmod{p^k}$. Therefore, $p^k \mid (x+1)(x-1)$. Since $(x+1) - (x-1) = 2$ and p is odd, we have that p can divide at most one of $x+1$ and $x-1$. Therefore, either $p^k \mid x+1$ or $p^k \mid x-1$. In particular, $x \equiv \pm 1 \pmod{p^k}$.

(b) As in (a), we have $2^k \mid (x+1)(x-1)$. Since $(x+1) - (x-1) = 2$, we have either $2^{k-1} \mid x+1$ and $2 \mid x-1$, or we have $2^{k-1} \mid x-1$ and $2 \mid x+1$. Hence, $x = t2^{k-1} \pm 1$, where $t \in \mathbf{Z}$. Modulo 2^k, there are four solutions given by $t = 0$ or 1, i.e., $x \equiv \pm 1$ or $\pm (1 + 2^{k-1}) \pmod{2^k}$.
When $k = 1$, the only solution is $x \equiv 1 \pmod 2$. When $k = 2$, the only solutions are $x \equiv \pm 1 \pmod 4$.