Math 110AH Homework 1

Nathan Solomon

October 11, 2023

Assignment due October 11th at 11:59 pm

1. Let $f : X \to Y$ and $g : Y \to Z$ be two maps. Prove that if f and g are injective (resp. surjective), then so is the composition $g \circ f$.

If f and g are both injective, then for any distinct elements $x_1, x_2 \in X, f(x_1) \neq f(x_2)$ because f is injective. Since g is also injective, $g(f(x_1)) \neq g(f(x_2))$, therefore $g \circ f$ is injective.

If f and g are both surjective, then for any element $z \in Z$, there exists an element $y \in Y$ such that $g(y) = z$, and there exists an element $x \in X$ such that $f(x) = y$. Since $g(f(x)) = z$, $g \circ f$ is surjective.

2. Prove that $(1 + 2 + \cdots + n)^2 = 1^3 + 2^2 + \cdots + n^3$.

First, I'll prove that $1+2+\cdots+n = (n^2+n)/2$. This is obvious in the base case ($n = 1$). If it's true for some positive integer n, then it must also be true for the $n + 1$ case, because

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

By induction, this implies the statement "$1+2+\cdots+n = (n^2+n)/2$" is true for any positive integer n.

The statement "$(1 + 2 + \cdots + n)^2 = 1^3 + 2^2 + \cdots + n^3$" is also obviously true in the base case ($n = 1$). If that statement is true for some positive integer n, it must also be true for $n + 1$, because

$$
\begin{aligned}
(1+2+\cdots+n+(n+1))^2 &= \left(\frac{n^2+n}{2}+(n+1)\right)^2 \\
&= \left(\frac{n^2+n}{2}\right)^2 + 2\cdot(n+1)\cdot\left(\frac{n^2+n}{2}\right)+(n+1)^2 \\
&= \left(\frac{n^4+2n^3+n^2}{4}\right)+(n^3+2n^2+n)+(n^2+2n+1) \\
&= \frac{n^4}{4}+\frac{3n^3}{2}+\frac{13n^2}{4}+3n+1 \\
&= \left(\frac{n^4}{4}+\frac{n^3}{2}+\frac{n^2}{4}\right)+(n^3+3n^2+3n+1) \\
&= \left(\frac{n^2+n}{2}\right)^2+(n+1)^3 \\
&= 1^3+2^3+\cdots+n^3+(n+1)^3
\end{aligned}
$$

So by induction, the statement $(1+2+\cdots+n)^2 = 1^3+2^2+\cdots+n^3$ must be true for any positive integer n.

Note that this whole proof works just as well if we choose $n=0$ to be the base case instead of $n=1$. Although the notation "$1+2+\cdots+n$" implies $n \geq 3$, the formula works for any $n \geq 0$.

3. Prove that 13 divides $14^n - 1$ for any $n \in \mathbb{N}$.

This is true in the base case ($n=1$), because $14^1 - 1 = 13$. If that statement is true for a natural number n, then there exists an integer z such that $13z = 14^n - 1$. Since $14^{n+1} - 1 = 14 \cdot 14^n - 1 = (13 \cdot 14^n) + (14^n - 1) = 13 \cdot (14^n + z)$, 13 must also divide $14^{n+1} - 1$. By induction, 13 divides $14^n - 1$ for any $n \in \mathbb{N}$.

Just like with the last question, this still works if we consider $\mathbb{N}$ to include zero.

4. Show that if $a^n - 1$ is prime and $n > 1$, then $a = 2$ and n is prime. If $2^n + 1$ is prime, what can you say about n?

For this question I will use $[x]$ to mean the equivalence class of x in $\mathbb{Z}/(a-1)\mathbb{Z}$.

Note that a cannot be zero or one, because if it were, $a^n - 1$ wouldn't be prime for any n. Since all prime numbers are positive, $a^n > 0$. If n is odd, that would not work when a is negative, and if n is even, $a^n = (-a)^n$, so we can assume without loss of generality that a is positive.

First, note that since $a = 1 + (a-1)$, $a = [1]$, which implies $a^n = [1]$, or equivalently, $a^n - 1 = [0]$.

$a^n - 1$ is prime, but now it also has to be divisible by $a - 1$. The only factors of a prime are $\pm$ itself and ± 1, so

$$a - 1 \in \{a^n - 1, 1 - a^n, 1, -1\}$$

We already ruled out the possibility that $a \leq 1$, which rules out the first option. If $a - 1 = 1 - a^n$, then $a^n - 1 = 1 - a$ is prime, but a is positive, so we can rule out the second option as well. The fourth option would imply $a = 0$, which we also already showed is not true, so we're left with the third option.

$$a = 2$$

Suppose there exists positive integers x, y such that $xy = n$. Then

$$\begin{aligned}
(2^x - 1) \times (1 + 2^x + 2^{2x} + \cdots + 2x(y-1)) &= \\
(2^x + 2^{2y} + 2^{3x} + \cdots + 2^{xy}) - (1 + 2^x + 2^{2x} + \cdots + 2^{x(y-1)}) &= \\
2^{xy} - 1 &= 2^n - 1
\end{aligned}$$

Therefore, if n is composite, then $2^n - 1$ has to be composite as well. Since that's not the case, n must be prime.

We can use a similar method to show that if $2^n + 1$ is prime, then n has to be a power of two. Suppose n is not a power of 2 – then there exist positive integers a and b such that b is odd, $b > 1$, and $n = b \times 2^a$. Let $x = 2^{(2^a)}$. Then

$$\begin{aligned}
(1 + x) \times \left(1 + (-x) + (-x)^2 + \cdots + (-x)^{b-1}\right) &= \\
\left(1 + (-x) + (-x)^2 + \cdots + (-x)^{b-1}\right) - \left((-x) + (-x)^2 + \cdots + (-x)^b\right) &= \\
1 - (-x)^b &= \\
1 + x^b &= \\
1 + \left(2^{(2^a)}\right)^b &= 2^n + 1
\end{aligned}$$

Therefore, if n is not a power of two, then $2^n + 1$ has to be composite. Since that's not the case, n must be a power of two.

5. Find all integer solutions of $93x + 39y = -6$.

Let $a = 93, b = 39, c = -6, d := (a, b) = 3, x_0 = -3, y_0 = 7$. Then using the results from question 6, the general solution is

$$(x, y) \in \{(-3 + 13k, 7 - 31k) : k \in \mathbb{Z}\} = \{\ldots, (-16, 38), (-3, 7), (10, -24), \ldots\}$$

6. Let a, b, c be non-zero integers and let $d = \gcd(a, b)$. Prove that the equation $ax + by = c$ has a solution x, y in integers if and only if $d|c$. Moreover, if $d|c$ and x_0, y_0 is a solution in integers then the general solution in integers is $x = x_0 + \frac{b}{d}k, y = y_0 - \frac{a}{d}k$ for all integers k.

Since $ax + by$ is a linear combination of a and b, which are both divisible by d, $ax + by$ must also be divisible by d, which is not possible unless d divides c.

We proved in class that a and b are coprime if and only if $ax + by = 1$ has a solution. Since a/d and b/d are coprime, we can let x' and y' be integer solutions to $ax'/d + by'/d = 1$. Then $x := x'cd$ and $y := y'cd$ are solutions to $ax + by = c$.

We have now proven that $ax + by = c$ has at least one solution $x, y \in \mathbb{Z}^2$ if and only if d divides c.

Suppose (x_0, y_0) and (x, y) are both solutions (not necessarily distinct). Then the difference between $ax_0 + by_0$ and $ax + by$ has to be zero, meaning that $a(x - x_0) = -b(y - y_0)$. Conversely, if $ax_0 + by_0 = c$ and $a(x - x_0) = -b(y - y_0)$ than it is obvious that $ax + by = c$. If we let $k = b(x - x_0)/d$, then substitute and rearrange, we get the following equations:

$$x = x_0 + \frac{bk}{d}$$
$$y = y_0 - \frac{ak}{d}$$

However, the only way x and y can both be integers is if k is an integer, so (x, y) is an integer solution to $ax+by = c$ if and only if there is exists an integer k that the two equations above are true for some pair of integers x_0, y_0 which already solve $ax_0 + by_0 = c$.

7. Show that if $a, b \in \mathbb{N}$, ab is the square of an integer, and $(a, b) = 1$, then a and b are squares.

Let p be any prime number that divides a, and let $d := p^n$ be the highest power of p that divides a. Then d is also the highest power of p that divides ab, because if it weren't, b would divide p, so the GCD of a and b would be at least p.

Let $p^{n'}$ be the highest power of p that divides $\sqrt{ab}$. Since $\left(p^{n'}\right)^2 = p^{2n'} = p^n$, we know that n must be an even number.

Let $a_1^{n_1} a_2^{n_2} \dots a_m^{n_m}$ be the prime factorization of a, where $a_1 < a_2 < \dots < a_m$. Repeating the above process for $p = a_1, a_2, \dots, a_m$ will show that all of the exponents $(n_1, n_2, \dots, n_m)$ are even.

Let $\sqrt{a} := a_1^{n_1/2} a_2^{n_2/2} \dots a_m^{n_m/2}$. Then $\sqrt{a}$ is an integer and $a = \sqrt{a}^2$, so a is a square.

Repeating the entire process above but with a replaced by b shows that b is also a square.

8. Prove that if $(a, n) = 1$ and $(b, n) = 1$, then $(ab, n) = 1$.

Suppose there is an integer $d > 1$ which divides both ab and n. Then since d divides ab, it must divide a or b. That means $(ab, n) > 1$ (or equivalently, $(ab, n) \neq 1$, since the GCD is always a positive integer) implies that $(a, n) \neq 1$ or $(b, n) \neq 1$. Conversely, if $(a, n) = 1$ and $(b, n) = 1$, then $(ab, n) = 1$.

9. Is $2^{10} + 5^{12}$ a prime? (Hint: use the identity $4x^4 + y^4 = (2x^2 + y^2)^2 - (2xy)^2$.)

Another way to see that $2^{10} + 5^{12}$ is not prime is to let $x = 4$ and let $y = 5^3$. Then

$$\begin{aligned}
2^{10} + 5^{12} &= 4x^4 + y^4 \\
&= (2x^2 + y^2)^2 - (2xy)^2 \\
&= (2x^2 + y^2 - 2xy) \cdot (2x^2 + y^2 + 2xy) \\
&= (32 + 15625 - 1000) \cdot (32 + 15625 + 1000) \\
&= 14657 \cdot 16657
\end{aligned}$$

which is actually the prime factorization of $2^{10} + 5^{12}$.

Question for the grader: If I had answered with just "No, because $2^{10}+5^{12} = 244141649 = 14657 \cdot 16657$", would I still get full points?

10. Show that there are infinitely many primes $p \equiv 2 \pmod 3$. (Hint: consider $3p_1p_2 \ldots p_n - 1$.)

For this question I will use $[n]$ to mean the equivalence class of n in $\mathbb{Z}/3\mathbb{Z}$, and $\mathbb{P}$ to mean the set of all prime numbers.

Suppose $P = \{p_1, p_2, \ldots, p_n\} = \mathbb{P} \cap [2]$ is a finite set of all the primes that are congruent to 2 (modulo 3). Then let $N = 3p_1p_2 \cdots p_n - 1$. For any $p_i \in P$, we know that p_i and N are coprime, because p_i is greater than one and N is one less than an integer multiple of p_i. Therefore N is coprime to every element of P.

Now consider the prime factorization of N. Every prime number in $[2]$ is in P, and N is not divisible by any element of P. Therefore N is the product of elements of $[0]$ and $[1]$, that is, there exists nonnegative integers a and b such that $[0]^a \times [1]^b = [2]$.

However, $[0] \times [0] = [0]$, $[1] \times [1] = [1]$, and $[0] \times [1] = [0]$. We have reached a contradiction, so there must be infinitely many primes in $\mathbb{P} \cap [2]$.