Homework 1

Warren Kim

October 11, 2023

Please grade my HW carefully. Thank you.

Question 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 $g \circ f$.

Response

Injective

Proof. Let f and g both be injective; i.e. $\forall x_1, x_2 \in X, f(x_1) = f(x_2) \implies x_1 = x_2$ and $\forall y_1, y_2 \in Y, g(y_1) = g(y_2) \implies y_1 = y_2$. Take any $x_1, x_2 \in X$. Then we have

$$\begin{aligned}
(g \circ f)(x_1) &= g(f(x_1)) \\
&= g(y_1) \\
&= g(y_2) && \text{Since } g \text{ is injective, } g(y_1) = g(y_2) \\
&= g(f(x_2)) && \text{Since } f \text{ is injective, } f(x_1) = f(x_2) \\
(g \circ f)(x_1) &= (g \circ f)(x_2)
\end{aligned}$$

□

Surjective

Proof. Let f and g both be surjective; i.e. $\forall y \in Y, \exists x \in X : y = f(x)$ and $\forall z \in Z, \exists y \in Y : z = g(y)$. Take any $z \in Z$. Then, we have

$$\begin{aligned}
(g \circ f)(x) &= g(f(x)) \\
&= g(y) && \text{Since } f \text{ is surjective, } y = f(x) \\
(g \circ f)(x) &= z && \text{Since } g \text{ is surjective, } z = g(y)
\end{aligned}$$

□

Question 2

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

Response

Proof. Let $P(n)$ be the statement: "$(1+2+\cdots+n)^2 = 1^3+2^3+\cdots+n^3$". We will induct on $n \in \mathbb{N}$.

(I) $P(1)$ reads "$1 = 1^3 = 1$ which is true.
(II) Assume $P(n)$ holds true for some $n \in \mathbb{N}$. We want to prove $P(n+1)$:

$$\begin{aligned}
1^3+2^3+\cdots+n^3+(n+1)^3 &= (1+2+\cdots+n)^2+(n+1)^3 \qquad \text{By the Inductive Hypothesis}\\
&= \left[\frac{n(n+1)}{2}\right]^2+(n+1)^3\\
&= \frac{n^2(n+1)^2}{4}+(n+1)(n+1)^2\\
&= \frac{n^2(n+1)^2}{4}+\frac{4(n+1)(n+1)^2}{4}\\
&= \frac{n^2(n+1)^2}{4}+\frac{4(n+1)(n+1)^2}{4}\\
&= \frac{(n^2+4n+4)(n+1)^2}{4}\\
&= \frac{(n+2)^2(n+1)^2}{4}\\
&= \left[\frac{(n+2)(n+1)}{2}\right]^2\\
1^3+2^3+\cdots+n^3+(n+1)^3 &= (1+2+\cdots+n)^2
\end{aligned}$$

So $P(n+1)$ is true, concluding the induction. $\square$

Question 3

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

Response

Proof. Let $P(n)$ be the statement: "13 divides $14^n - 1$ for any $n \in \mathbb{N}$". We will induct on $n \in \mathbb{N}$.

(I) $P(1)$ reads "$13 \mid (14^1 - 1) = 13$" which is true.
(II) Assume $P(n)$ holds true for some $n \in \mathbb{N}$. We want to prove $P(n+1)$. Recall that $13 \mid (14^n - 1)$ can be expressed as $14^n - 1 = 13q \iff 14^n = 13q + 1$ where $q \in \mathbb{Z}$.

$$\begin{aligned}
14^{n+1} - 1 &= (14 \cdot 14^n) - 1 \\
&= (14 \cdot [13q + 1]) - 1 && \text{By the Inductive Hypothesis} \\
&= 182q + 14 - 1 \\
&= 182q + 13 \\
&= 13(14q + 1) \\
14^{n+1} - 1 &= 13p && \text{Let } p = 14q + 1
\end{aligned}$$

So $P(n+1)$ is true, concluding the induction. □

Question 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?

Response

Proof. Note that $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$.

Let $n > 1$. Then, we have

$$\begin{aligned} a^n - 1 &= (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1) \\ &\implies (a-1) \mid (a^n - 1) \end{aligned}$$

But $a^n - 1$ is prime $\implies a - 1 = 1$ so $a = 2$.

Now assume by contradiction that n is composite; i.e. $n = pq$ for some $1 < p, q < n$. Then we get

$$\begin{aligned} a^{pq} - 1 &= (a^p)^q - 1 \\ &= (a^p - 1)([a^p]^{q-1} + [a^p]^{q-2} + \cdots + a^p + 1) \end{aligned}$$

So $a^n - 1$ is composite, a contradiction. Therefore, n must be prime. $\square$

If $2^n + 1$ is prime, then n must be either 0 or a power of 2.

Question 5

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

Response

$a = 93, b = 39$

$$\begin{aligned}
93 &= 2(39) + 15 \iff 15 = 93 - 2(39) \\
39 &= 2(15) + 9 \iff 9 = 39 - 2(15) \\
15 &= 1(9) + 6 \iff 6 = 15 - 1(9) \\
9 &= 1(6) + 3 \iff 3 = 9 - 1(6) \\
6 &= 2(3) + 0
\end{aligned}$$

So $(93, 39) = 3$. Then,

$$\begin{aligned}
3 &= 9 - 1(6) \\
&= 9 - 1[15 - 1(9)] \\
&= 2(9) - 15 \\
&= 2[39 - 2(15)] - [93 - 2(39)] \\
&= 4(39) - 4(15) - 93 \\
&= 4(39) - 4[93 - 2(39)] - 93 \\
&= 12(39) - 5(93) \\
3 &= 39(12) - 93(5) \\
-6 &= 93(10) + 39(-24) && \text{Multiply both sides by } -2
\end{aligned}$$

Then we get $x = 10 - 13k, y = -24 + 31k$ where $k \in \mathbb{Z}$ (from **Question 6**) to be all the integer solutions of $93x + 39y = -6$.

Question 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 $d \mid c$. Moreover, if $d \mid c$ 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.

Response

(i)

Proof. ($\implies$) Let $d = \gcd(a, b)$ and $ax + by = c$ have solutions $x, y \in \mathbb{Z}$. Since $d \mid a, b$, we can write $a = dp, b = dq$ for some $p, q \in \mathbb{Z}, p \neq q$. Now, use the assumption that $ax+by = c$ has integer solutions x, y to get:

$$
\begin{aligned}
c &= ax + by && \\
&= (dp)x + (dq)y && \text{Substitute } a, b \\
&= d(px + qy) && \text{Factor } d \\
c = dr &\iff d \mid c && \text{Let } r = px + qy
\end{aligned}
$$

Here, $r \in \mathbb{Z}$ because $x, y, p, q \in \mathbb{Z}$ and the integers are closed under addition and multiplication. So $d \mid c$.

($\impliedby$) Let $d \mid c$. Then by definition, $c = dq$ for some $q \in \mathbb{Z}$. Using Bezout's Identity, we have

$$
\begin{aligned}
ax' + by' &= d && \\
(ax' + by')q &= dq && \text{Multiply both sides by } q \\
a(x'q) + b(y'q) &= c && c = dq \\
ax + by &= c && \text{Let } x = x'q, y = y'q
\end{aligned}
$$

Here, $x, y \in \mathbb{Z}$ because $x', y', q \in \mathbb{Z}$ and the integers are closed under multiplication. Thus, $ax+by = c$ has integer solutions. $\square$

(ii)

Proof. Let $d \mid c$ and x_0, y_0 be integer solutions. Using Bezout's Identity, we get $a = dp, b = dq$ for some $p, q \in \mathbb{Z}, p \neq q$. Then we have: $ax_0 + by_0 = c = ax + by$:

$$
\begin{aligned}
ax_0 + by_0 &= ax + by && \\
a(x - x_0) &= b(y_0 - y) && \\
dp(x - x_0) &= dq(y_0 - y) && \text{Substitute } a, b \\
p(x - x_0) &= q(y_0 - y) &&
\end{aligned}
$$

Since $\gcd(p, q) = 1$, it must be true that $p \mid (y_0 - y)$ (similarly, $q \mid (x - x_0)$). That is:

$$
\begin{aligned}
y_0 - y &= pk && k \in \mathbb{Z} \\
y &= pk + y_0 && \\
y &= y_0 - \frac{a}{d}k && \text{Substitute } p
\end{aligned}
$$

and

$$
\begin{aligned}
x - x_0 &= qk && k \in \mathbb{Z} \\
x &= x_0 + qk && \\
x &= x_0 + \frac{b}{d}k && \text{Substitute } q
\end{aligned}
$$

Therefore, the general solution in integers is $x = x_0 + \frac{b}{d}k$ and $y = y_0 - \frac{a}{d}k$ for all integers k.

$\square$

Question 7

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

Response

Proof. Note that $x = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$ is a square $\iff$ $k_1, k_2, \dots, k_n$ are all even. **(i)**

Let $a, b \in \mathbb{N}$, $p \in \mathbb{Z}$ such that $p^2 = ab$ and $(a, b) = 1$. Then, we can write both a and b in their unique prime factorizations (from the Fundamental Theorem of Arithmetic) as:

$$a = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$$

$$b = q_1^{s_1} q_2^{s_2} \dots q_m^{s_m}$$

Then, we have:

$$p^2 = ab = (p_1^{k_1} p_2^{k_2} \dots p_n^{k_n})(q_1^{s_1} q_2^{s_2} \dots q_m^{s_m})$$

Since $(a, b) = 1$ (i.e. a and b have no common divisor) and ab is a square, by **(i)**, $k_1, k_2, \dots, k_n$ and $s_1, s_2, \dots, s_n$ are all even $\implies$ a and b are squares, respectively. $\square$

Question 8

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

Response

Proof. Let $a, b, n \in \mathbb{Z}$. First we use the Bezout Identity for a and b:

$$ax + ny = 1$$

$$bx' + ny' = 1$$

where $x, x', y, y' \in \mathbb{Z}$. Then we have:

$$\begin{aligned}
(ax + ny)(bx' + ny') &= (ax)(bx') + (ax)(ny') + (ny)(bx) + (ny)(ny') \\
&= ab(xx') + n(axy' + bxy + nyy') \\
&= (ab)p + nq = 1 && \text{Let } p = xx', q = axy' + bxy + nyy'
\end{aligned}$$

Here, p is an integer because $x, x' \in \mathbb{Z}$ and integers are closed under multiplication. Analogously, q is an integer because $a, x, x', b, y, y', n \in \mathbb{Z}$ are integers, and integers are closed under addition. Now, we reverse the Bezout Identity to get

$$(ab)p + nq = 1 \iff (ab, n) = 1$$

$\square$

Question 9

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

Response

The number $2^{10}+5^{12}$ is not prime.

Proof. Let $x=2^2=4, y=5^3=125$. Then,

$$\begin{aligned}
2^{10}+5^{12} &= 2^2\cdot 2^8+5^{12}\\
&= 4(2^2)^4+(5^3)^4\\
&= 4x^4+y^4\\
&= (2x^2+y^2)^2-(2xy)^2\\
&= (2x^2+y^2+2xy)(2x^2+y^2-2xy)\\
&= (2[4]^2+[125]^2+2[4][125])(2[4]^2+[125]^2-2[4][125])\\
&= (32+15625+1000)(32+15625-1000)\\
&= (16657)(14657)
\end{aligned}$$

Since $2^{10}+5^{12}$ can be represented as the product of two integers that are both greater than 1, it is composite and therefore not prime. $\square$

Question 10

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

Response

Proof. Assume by contradiction that we have an ordered finite set $S = \{p_1, p_2, \dots, p_n\}$ of primes of the form $p \equiv 2 \ (mod\ 3)$ where $n \in \mathbb{N}$. Let $N = 3p_1p_2 \dots p_n - 1$. Then there are two cases:

(i) N is prime: If N is prime, then we are done since $N \equiv 2 \ (mod\ 3)$ and is greater than any element in S, a contradiction.

(ii) N is composite: If N is composite, then by the Fundamental Theorem of Arithmetic, N has a unique prime factorization. Clearly, N cannot be congruent to $0 \ (mod\ 3)$ since N takes the form $3k - 1$. If N is a product of primes all congruent to $1 \ (mod\ )3$, then N must be congruent to $1 \ (mod\ 3)$ $([1] \cdot [1] \cdot \ldots \cdot [1] \equiv [1])$. However, Since $N \equiv 2 \ (mod\ 3)$, this cannot be true. Therefore, there should be at least one prime congruent to $2 \ (mod\ 3)$ as a factor of N.

□