# M 328K: Homework 1

Katherine Ho

September 10, 2024

1. Show that $(3!)^n \mid (3n)!$ for all $n \geq 0$.

*Proof by Induction.* We aim to show that

$$(3n)! = (3!)^n \cdot k \text{ for some } k \in \mathbb{Z}.$$

Base case ($n = 0$): $0! = (3!)^0 \cdot k,\ k = 1$
Base case ($n = 1$): $3! = (3!) \cdot k,\ k = 1$

Inductive Hypothesis: Assume that $(3n)! = (3!)^n \cdot k$ is true for some $k \in \mathbb{Z}$ and all $n \geq 0$.
Consider $n + 1$:

$$\begin{aligned}(3(n+1))! &= (3n+3)! \\ &= (3n+3)(3n+2)(3n+1)(3n)! \\ &= (3n+3)(3n+2)(3n+1)(3!)^n \cdot k && \text{By the IH}\end{aligned}$$

**Lemma 1.** *The product of any two consecutive integers is even.*

We want to show that $n(n+1)$ is even $\forall n \in \mathbb{Z}$.

(a) Case 1: n is even. We have $n = 2a$, where $a \in \mathbb{Z}$.

$$n(n+1) = 2a(2a+1) = 2(2a^2 + a)$$

$2a^2 + a \in \mathbb{Z}$, thus n(n+1) is even.

(b) Case 2: n is odd. We have $n = 2b + 1$, where $b \in \mathbb{Z}$.

$$\begin{aligned}n(n+1) &= (2b+1)(2b+1+1) \\ &= 4b^2 + 6b + 2 \\ &= 2(2b^2 + 3b + 1)\end{aligned}$$

$2b^2 + 3b + 1 \in \mathbb{Z}$, thus $n(n+1)$ is even.

The statement is true in both cases. Therefore, the product of any two consecutive integers is even.

By Lemma 1: $(3n+2)(3n+1) = 2p$ for some $p \in \mathbb{Z}$.

$$\begin{aligned}(3(n+1))! &= (3n+3)(2p)(3!)^n \cdot k \\ &= 3(n+1)(2)(p)(3!)^n \cdot k \\ &= (3!)^{n+1} \cdot ((n+1) \cdot p \cdot k)\end{aligned}$$

where $(n+1) \cdot p \cdot k \in \mathbb{Z}$. Hence

$$(3(n+1))! = (3!)^{n+1} \cdot k$$

Thus $(3!)^n \mid (3n)!$ for all $n \geq 0$.

$\square$

2. Show that if $a$ and $b$ are odd integers, then $8 \mid a^2 - b^2$.

*Proof.* We aim to show that $a^2 - b^2 = 8k,$ for some $k \in \mathbb{Z}$.
Given a and b are odd integers, they can be rewritten as $a = 2m+1$ and $b = 2n+1$ for some $m, n \in \mathbb{Z}$.

Then, we have

$$\begin{aligned} a^2 - b^2 &= (2m+1)^2 - (2n+1)^2 \\ &= 4m^2 + 4m + 1 - (4n^2 + 4n + 1) \\ &= 4(m(m+1) - n(n+1)) \end{aligned}$$

By Lemma 1: $4(m(m+1) - n(n+1)) = 4(2r - 2s)$ for some $r, s \in \mathbb{Z}$.

$$4(2r - 2s) = 8(r - s)$$

We now have $a^2 - b^2 = 8(r - s)$, where $r - s$ is an integer.
Thus if $a$ and $b$ are odd integers, then $8 \mid a^2 - b^2$.

□

3. Consider the following sequence of integers:

$$11, 111, 1111, \ldots$$

(a) Show by induction that each integer in the sequence can be written in the form $4k + 3$.

*Proof by Induction.* Each element in the sequence can be described with:

$$x_n = \sum_{i=0}^{n+1} 10^i$$

Let $P(n)$ be the statement that $x_n$ can be written in the form $4k + 3$.

Base case: $P(0)$

$$x_0 = \sum_{i=0}^{0+1} 10^i = 10^0 + 10^1 = 11 = 4(2) + 3, \text{ where } 2 \in \mathbb{Z}$$

Inductive Hypothesis: Assume $P(n)$ is true. That is,

$$x_n = \sum_{i=0}^{n+1} 10^i = 4k + 3 \text{ for some } k \in \mathbb{Z}$$

$P(n+1)$:

$$\begin{aligned} x_{n+1} &= \sum_{i=0}^{(n+1)+1} 10^i \\ &= 10^{n+2} + \sum_{i=0}^{n+1} 10^i \\ &= 10^{n+2} + 4k + 3 && \text{By the IH} \\ &= 100 \cdot 10^n + 4k + 3 \\ &= 4(25 \cdot 10^n + k) + 3 \end{aligned}$$

where $(25 \cdot 10^n + k) \in \mathbb{Z}$. Thus $P(n+1)$ is true, proving that each integer in the sequence can be written in the form $4k + 3$.

□

(b) Use the previous result together with the division algorithm to show that no integer in the sequence is a perfect square.

*Proof by Contradiction.* Given that each integer in the sequence can be written as $4k+3$, suppose that each integer can be written as a perfect square. That is,

$$4k + 3 = a^2, a \in \mathbb{Z}$$

i. Case 1: a is odd, ie. $a = 2p + 1, p \in \mathbb{Z}$

$$\begin{aligned} 4k + 3 &= (2p + 1)^2 \\ &= 4p^2 + 4p + 1 \\ &= 4(p^2 + p) + 1 \end{aligned}$$

By the division algorithm, $\exists$ integers $q$ and $r$ such that $a = bq + r$. In this instance, $q = 4$ and $r = 3$. If a is an odd integer, $r = 1$, a contradiction.

ii. Case 2: a is even, ie. $a = 2p, p \in \mathbb{Z}$

$$\begin{aligned} 4k + 3 &= (2p)^2 \\ &= 4(p^2) \end{aligned}$$

If a is an even integer, $r = 0$, a contradiction.

The supposition is false, thus no integer in the sequence is a perfect square. □

4. Let $a$ and $b$ be coprime integers. Show that $ab$ and $a + b$ are also coprime.

*Proof.* The contrapositive of the given statement is as follows:

"If $ab$ and $a + b$ are not coprime, then $a$ and $b$ are not coprime."

Suppose that $ab$ and $a + b$ are not coprime. That is, suppose $d|ab$ and $d|a + b$, for some $d \in \mathbb{Z}$. Given that $a$ and $b$ are coprime,

$$d|ab \implies d|a \text{ OR } d|b$$

Say $d|a$. This implies that $a = dc$ for some $c \in \mathbb{Z}$.
Next, we have

$$\begin{aligned} d|a + b \implies a + b &= dk \text{ for some } k \in \mathbb{Z} \\ b &= dk - a \\ b &= dk - dc \\ b &= d(k - c) \end{aligned}$$

This suggests that $a$ and $b$ are not coprime due to sharing a common factor $d$. Thus the contrapositive statement is true and so the given statement is true.

□

5. Prove the following properties of the greatest common divisor (without appealing to prime factorization):

(a) If $\gcd(a, b) = \gcd(a, c) = 1$, then $\gcd(a, bc) = 1$.

*Proof.* We want to show that $ax + bcy = 1$ for some $x, y \in \mathbb{Z}$. Given $\gcd(a, b) = \gcd(a, c) = 1$ and Bezout's Theorem, we can write

$$ax_1 + by_1 = ax_2 + cy_2 = 1 \text{ for some } x_1, y_1, x_2, y_2 \in \mathbb{Z}$$

i. Multiply the first expression by c. We get

$$\begin{aligned} acx_1 + bcy_1 &= c \\ a(cx_1) + bc(y_1) &= c \end{aligned}$$

ii. Multiply the second expression by b. We get

$$\begin{aligned} abx_2 + bcy_2 &= c \\ a(bx_2) + bc(y_2) &= c \end{aligned}$$

Now, we have

$$a(cx_1) + bc(y_1) = a(bx_2) + bc(y_2) = c$$

Since $ax_1 + by_1 = ax_2 + cy_2 = 1$,

$$a(cx_1) + bc(y_1) = a(bx_2) + bc(y_2) = 1$$

Thus, $ax + bcy = 1$ and $\gcd(a, bc) = 1$. □

(b) If $\gcd(a, b) = 1$, then $\gcd(ac, b) = \gcd(c, b)$.

*Proof.* Suppose $\gcd(ac, b) = z_1$ and $\gcd(c, b) = z_2$. We have

$$\begin{aligned} ac(x_1) + b(y_1) &= z_1 \\ c(x_2) + b(y_2) &= z_2 \end{aligned}$$

Given $ax + by = 1$ for some $x, y \in \mathbb{Z}$, we have

i. $axz_1 + byz_1 = z_1$

$$\begin{aligned} ax(ac(x_1) + b(y_1)) + byz_1 &= z_1 \\ c(a^2xx_1) + b(axy_1 + y_1z_1) &= z_1 \end{aligned}$$

$\therefore z_2 | z_1$ since $z_2$ can divide any linear combination of c and b.

ii. $axz_2 + byz_2 = z_2$

$$\begin{aligned} ax(cx_2 + by_2) + by(z_2) &= z_2 \\ ac(xx_2) + b(axy_2 + yz_2) &= z_2 \end{aligned}$$

$\therefore z_1 | z_2$ since $z_2$ can divide any linear combination of ac and b.

Now, we have $z_1 | z_2$ and $z_2 | z_1$.

**Lemma 2.** *For some integers $x_1, x_2 \in \mathbb{Z}$, if $x_1 | x_2$ and $x_2 | x_1$, then $x_1 = x_2$ or $x_1 = -x_2$.*

Given $x_1 | x_2$ and $x_2 | x_1$, we have

$$\begin{aligned} x_2 &= x_1 \cdot a \text{ for some } a \in \mathbb{Z} \\ x_1 &= x_2 \cdot b \text{ for some } b \in \mathbb{Z} \\ x_1 &= (x_1 \cdot a) \cdot b \\ 1 &= a \cdot b \end{aligned}$$

This tells us $a = b = 1$ or $a = b = -1$.

i. $a = b = 1 \implies x_1 = x_2$

ii. $a = b = -1 \implies x_1 = -x_2$

Thus if $x_1 | x_2$ and $x_2 | x_1$, then $x_1 = x_2$ or $x_1 = -x_2$.

By Lemma 2, $z_1 = z_2$ since $z_1$ and $z_2$ both must be positive integers.
Thus $\gcd(ac, b) = \gcd(c, b)$. □

(c) If $\gcd(a, b) = 1$, $d|ac$, and $d|bc$, then $d|c$.

*Proof.* Given $d|ac$ and $d|bc$, we have

$$ac = dp \text{ for some } p \in \mathbb{Z}$$
$$bc = dq \text{ for some } q \in \mathbb{Z}$$

Given a and b are coprime, we have

$$\begin{aligned} ax + by &= 1 \text{ for some } x, y \in \mathbb{Z} \\ acx + bcy &= c \\ dpx + dqy &= c \\ d(px + qy) &= c \end{aligned}$$

Since $x, y, p, q, \in \mathbb{Z}$, $d|c$. □

(d) If $\gcd(a, b) = 1$, then $\gcd(a^2, b^2) = 1$.

*Proof.* Given a and b are coprime, there exist some $x, y \in \mathbb{Z}$ such that $ax + by = 1$.

$$\begin{aligned} 1 &= ax + by \\ 1^3 &= (ax + by)^3 \\ 1 &= (ax + by)^2 \cdot (ax + by) \\ 1 &= (a^2x^2 + 2axby + b^2y^2) \cdot (ax + by) \\ 1 &= a^3x^3 + a^2x^2by + 2a^2x^2by + 2axb^2y^2 + b^2y^2ax + b^3y^3 \\ 1 &= a^2(ax^3 + x^2by + 2x^2by) + b^2(2axy^2 + y^2ax + by^3) \end{aligned}$$

This equation can be rewritten as

$$a^2x_1 + b^2y_2 = 1$$

where

$$\begin{aligned} x_1 &= ax^3 + x^2by + 2x^2by \in \mathbb{Z} \\ y_1 &= 2axy^2 + y^2ax + by^3 \in \mathbb{Z} \end{aligned}$$

Therefore, by Bezout's Theorem, $\gcd(a^2, b^2) = 1$. □

6. Use the Euclidean Algorithm to obtain integers $x$ and $y$ satisfying

$$119x + 272y = \gcd(119, 272)$$

$$\begin{aligned} 272 &= 2 \cdot 119 + 34 \\ 119 &= 3 \cdot 34 + 17 \\ 34 &= 2 \cdot 17 + 0 \end{aligned}$$

$$\boxed{GCD = 17}$$

$$\begin{aligned} 17 &= 119 - 3 \cdot 34 \\ &= 119 - 3(272 - 2 \cdot 119) \\ &= 119 - (3 \cdot 272) + 6(119) \\ &= 7(119) - 3(272) \end{aligned}$$

$$\boxed{x = 7,\ y = -3}$$