

1. Show that, if m is an odd integer, then $m^2 \equiv 1 \pmod{8}$.

Solution: Since m is odd $\exists b \in \mathbb{Z}$ such that $m = 2b + 1$.

Now $(2b + 1)^2 = 4b^2 + 4b + 1 = 4b(b + 1) + 1$.

Observe that $b(b + 1)$ must be even, for if b is odd then $b + 1$ is even.

Otherwise b is even.

Hence $\exists d \in \mathbb{Z}$ such that $b(b + 1) = 2d$.

Consequently, $(2b + 1)^2 = 4b^2 + 4b + 1 = 4(2d) + 1 = 8d + 1$.

Finally, $m^2 = 8d + 1 \equiv 1 \pmod{8}$

2. Find $3^{2015} \pmod{23}$

Solution: We first compute a sequence of the form $3^n \pmod{23}$ where n is a power of 3, viz:

$$3^2 = 9 \pmod{23}$$

$$3^4 \equiv 12$$

$$3^8 \equiv 6$$

$$3^{16} \equiv 13$$

$$3^{32} \equiv 8$$

$$3^{64} \equiv 18$$

$$3^{128} \equiv 2$$

$$3^{256} \equiv 4$$

$$3^{512} \equiv 16$$

$$3^{1024} \equiv 3$$

Now $2015 = 1024 + 512 + 256 + 128 + 64 + 16 + 8 + 4 + 2 + 1$. It follows that:

$$3^{2015} = (3^{1024})(3^{512})(3^{256})(3^{128})(3^{64})(3^{16})(3^8)(3^4)(3^2)(3^1)$$

$$\text{So, mod } 23, 3^{2015} \equiv (3)(16)(4)(2)(18)(13)(6)(12)(9)(3) =$$

$$(48)(4)(36)(78)(108)(3) \equiv (2)(4)(13)(9)(16)(3) = (104)(9)(48) \equiv (12)(9)(2) = (24)(9)$$

$$\equiv 9 \pmod{23}$$

3. Three pirates and a monkey are marooned on an island. The pirates have collected a pile of coconuts that they plan to divide equally among themselves the next morning. Not trusting his comrades, one of the group wakes up during the night and divides the coconuts into three equal parts with one left over, which s/he gives to the monkey. He then hides his portion of the pile. During the night, each of the other two pirates does exactly the same thing by dividing the pile s/he finds into three equal parts, leaving one coconut for the monkey and hiding his portion. In the morning, the pirates gather and split the remaining pile of coconuts into three parts and one is left over for the monkey. What is the minimum number of coconuts the pirates have collected for their original pile?

(Note: you cannot use any theorems that we have not studied yet in your solution to this problem.)

Extra Credit: Same question except four pirates instead of three?

Solution: Suppose that there are n coconuts when the pirates retire for the night.

When the first pirate awakens, s/he gives 1 coconut to the monkey and leaves $2/3$ of the remaining coconuts.

Hence when the first pirate goes back to bed, there are $(2/3)(n - 1)$ coconuts remaining.

When the second pirate awakens, s/he gives 1 coconut to the monkey and leaves $2/3$ of the remaining coconuts.

So, when the second pirate returns to bed, there are $(2/3) \{ (2/3)(n - 1) - 1 \} = (4n - 10)/9$ coconuts remaining.

When the third pirate awakens, s/he gives 1 coconut to the monkey and leaves $2/3$ of the remaining coconuts.

So, when the third pirate returns to bed, there are $(2/3) ((4n - 10)/9 - 1) = (8n - 38)/27$ coconuts left.

Finally, the pirates all awaken, give one coconut to the monkey and split the remaining coconuts three ways.

So $(8n - 38)/27$ must be an integer that is congruent to 1 (mod 3).

$$\begin{aligned} \text{Now } 8n &\equiv 38 \pmod{27} \implies 8n \equiv 11 \pmod{27} \implies 80n \equiv 110 \pmod{27} \\ &\implies -n \equiv 2 \pmod{27} \implies n \equiv -2 \pmod{27} \end{aligned}$$

We consider the positive solutions to this congruence: $n = 25, 52, 79, 96, \dots$

If $n = 25$, then $(8(25) - 38) / 27 = 6$ is *not* congruent $1 \pmod{3}$

If $n = 52$, then $(8(52) - 38) / 27 = 14$ is *not* congruent $1 \pmod{3}$

If $n = 79$, then $(8(79) - 38) / 27 = 22 \equiv 1 \pmod{3}$

Thus $n = 79$ is the smallest number of coconuts that could have been in the original collection.

4. Let X be the set of members of the Cartesian product $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$.
 Let Y be the set of all 2×2 matrices with integer entries.
 Assume that addition in X satisfies the usual rule (for vector addition), namely $(a, b, c, d) + (e, f, g, h) = (a+e, b+f, c+g, d+h)$ and that Y satisfies the usual rules of matrix addition, namely:

$$\begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} + \begin{bmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{bmatrix} = \begin{bmatrix} c_{11} + d_{11} & c_{12} + d_{12} \\ c_{21} + d_{21} & c_{22} + d_{22} \end{bmatrix}$$

Define a function $F: X \rightarrow Y$ as follows:

$$F(a, b, c, d) = \begin{bmatrix} a & 2b \\ 3c & 4d \end{bmatrix}$$

- (1) Is F well-defined?
- (2) Is F injective?
- (3) Is F surjective?
- (4) Is F bijective?
- (5) Is F an isomorphism?

Of course, justify each answer!

Solution: (1) F is well-defined because each output is unambiguous and lies in Y .

(2) F is injective:

Suppose that $F(a, b, c, d) = F(a', b', c', d')$

Then by definition of F we obtain:

$\begin{bmatrix} a & 2b \\ 3c & 4d \end{bmatrix} = \begin{bmatrix} a' & 2b' \\ 3c' & 4d' \end{bmatrix}$. Now two matrices are equal if and only corresponding

entries are equal. So

$$a = a', \quad b = b', \quad c = c' \text{ and } d = d'$$

Hence $(a, b, c, d) = (a', b', c', d')$

(3) F is not surjective:

Clearly $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in Y$

But this point is not in the range of F , for if it were, then $2b = 1$. This has no solution in the set of integers.

(4, 50) Of course, it follows that F cannot be bijective nor can it be an isomorphism.

5. Using mathematical induction, prove that $\left(\frac{1}{2}\right)\left(\frac{3}{4}\right) \dots \frac{2n-1}{2n} \leq \frac{1}{\sqrt{3n+1}}$ for $n \geq 1$.

Solution:

For $n \geq 1$, let H_n represent the statement $\left(\frac{1}{2}\right)\left(\frac{3}{4}\right) \dots \frac{2n-1}{2n} \leq \frac{1}{\sqrt{3n+1}}$

Base case: $n = 1$: LHS = $\frac{1}{2}$; RHS = $1/\sqrt{3+1} = 1/2$

And so H_1 is satisfied.

Before completing the inductive step we first prove the inequality:

$$\text{Lemma: } \frac{2n+1}{2n+2} \leq \frac{\sqrt{3n+1}}{\sqrt{3n+4}} \quad \forall n \in \mathbb{N} \quad (**)$$

Proof of lemma:

Clearly $19n < 20n$ for all $n \in \mathbb{N}$

$$\text{So: } 4 + 19n + 28n^2 + 12n^3 < 4 + 20n + 28n^2 + 12n^3$$

$$\text{Factoring: } (2n+1)^2(3n+4) < (2n+2)^2(3n+1)$$

Basic algebra: $\frac{(2n+1)^2}{(2n+2)^2} < \frac{3n+4}{3n+1} \quad \forall n \in \mathbb{N}$

Which yields the result that we seek:

$$\frac{2n+1}{2n+2} \leq \frac{\sqrt{3n+1}}{\sqrt{3n+4}} \quad \forall n \in \mathbb{N}$$

Next we proceed to the induction step.

Inductive step: Let $n \geq 1$ be given. Assume that H_n is true, that is:

$$(*) \quad \left(\frac{1}{2}\right)\left(\frac{3}{4}\right) \cdots \left(\frac{2n-1}{2n}\right) \leq \frac{1}{\sqrt{3n+1}}$$

Using the inductive hypothesis (*), we obtain:

$$\left(\left(\frac{1}{2}\right)\left(\frac{3}{4}\right) \cdots \left(\frac{2n-1}{2n}\right)\right) \left(\frac{2(n+1)-1}{2(n+1)}\right) \leq \frac{1}{\sqrt{3n+1}} \frac{2n+1}{2n+2}$$

$$(\text{invoking Lemma **}) \leq \frac{1}{\sqrt{3n+1}} \frac{\sqrt{3n+1}}{\sqrt{3n+4}} = \frac{1}{\sqrt{3n+4}} = \frac{1}{\sqrt{3(n+1)+1}}$$

Thus H_{n+1} has been proven.