Mid II – Solutions

Q1]. . . [20 points] State the Principle of Induction.

Suppose $P(n)$ is a statement involving natural numbers n.

- $P(1)$ true
- $\forall k\,(P(k) \text{ true} \rightarrow P(k+1) \text{ true})$

$\longrightarrow (\forall n \in \mathbb{N})\ P(n)$ true.

Give a proof by induction of the following statement.

call this statement $P(n)$.

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6} \qquad \text{for all } n \in \mathbb{N}.$$

$P(1)$ is true. $\quad 1^2 = 1 \overset{??}{=} \frac{1(1+1)(2(1)+1)}{6} = \frac{1(2)(3)}{6} = \frac{6}{6} = 1$

So $P(1)$ is true..

$P(k)$ true $\rightarrow P(k+1)$ true. Assume $P(k)$ true. That is

$$1^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6} \qquad \longrightarrow (*)$$

Then $1^2 + \cdots + (k+1)^2 = (1^2 + \cdots + k^2) + (k+1)^2$

$$= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \qquad \text{by } (*)$$

$$= \frac{(k+1)(2k^2+k) + 6(k+1)^2}{6}$$

$$= \frac{(k+1)(2k^2+k+6k+6)}{6}$$

$$= \frac{(k+1)(k+2)(2k+3)}{6} \qquad 2k^2+7k+6 = (k+2)(2k+3)$$

$$= \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6}$$

Thus $P(k+1)$ true.

By the Principle of Induction $P(n)$ is true for all $n \in \mathbb{N}$.

Q2]... [20 points] Give a proof of the following statement.
If a natural number n is not a perfect cube (that is n is not one of $1, 8, 27, 64, \ldots$), then its cube root $\sqrt[3]{n}$ is irrational.

Proof We argue by contradiction. Assume to the contrary that $\sqrt[3]{n}$ is rational. This means $\sqrt[3]{n} = \frac{a}{b}$ for some $a, b \in \mathbb{N}$.

$$\Rightarrow \quad n = \frac{a^3}{b^3} \quad \Rightarrow \quad \boxed{b^3 n = a^3} \quad \text{—(*)}.$$

Now the existence portion of F.T.A. tells us that

$$n = p_1^{l_1} \cdots p_k^{l_k} \quad \text{where } p_i \text{ are distinct primes and } l_i \in \mathbb{N}.$$

The hypothesis that n is not a perfect cube means that $l_j \not\equiv 0 \bmod 3$ for some $1 \le j \le k$.

Substituting into (*) gives $\boxed{b^3 p_1^{l_1} \cdots p_j^{l_j} \cdots p_k^{l_k} = a^3}$ —(**)

Note that the number of occurences of p_j on the Left side of (**) $\not\equiv 0 \bmod 3$. (Note p_j may occur in the prime factorization of b, but the exponent 3 in b^3 ensures that the total number of p_j's on Left side of (**) is still $\not\equiv 0 \bmod 3$)

Note that the number of occurences of p_j on the right side of (**) $\equiv 0 \bmod 3$, because of the exponent 3 in a^3.

But these last 2 facts contradict uniqueness in the F.T.A. for the integer a^3.

This contradiction arose from the assumption that $\sqrt[3]{n}$ is rational.

Thus $\sqrt[3]{n}$ is irrational. ∎

Q3]... [20 points] Compute $\gcd(729, 354)$ and find integers c and d such that

$$729c + 354d = \gcd(729, 354).$$

$729 = 354(2) + 21$
$354 = 21(16) + 18$
$21 = 18(1) + 3$
$18 = 3(6) + 0$

$\Rightarrow \boxed{\gcd(729, 354) = 3}$

Moreover...

$3 = 21 + 18(-1) = 21 + (354 + 21(-16))(-1)$
$= 21(17) + 354(-1)$
$= (729 + 354(-2))17 + 354(-1)$
$= 729(17) + 354(-35)$

$\boxed{c = 17}$ $\boxed{d = -35}$

Rough Work

729 − 708 = 21 ← 354 = 2 × 708

21 × 16 = 126, 21 × 336 → 354 − 336 = 18

Recall that the Fibonacci numbers are defined by $F_1 = 1 = F_2$ and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 3$. Give a proof of the following statement.

$$\gcd(F_n, F_{n-1}) = 1 \qquad \text{for all integers } n \geq 2.$$

Prove the statement $P(n)$: $\gcd(F_n, F_{n-1}) = 1$ true $\forall n \geq 2$.

Base case $n = 2$ $\gcd(F_2, F_1) = \gcd(1, 1) = 1$. True ✓.

Assume $\gcd(F_k, F_{k-1}) = 1$

Now $F_{k+1} = F_k + F_{k-1}$ ---- def^n of Fibo...

Euc. Alg. $\Rightarrow$ $\gcd(F_{k+1}, F_k) = \gcd(F_k, F_{k-1})$
$= 1$ by Ind. hypoth.

$\Rightarrow \gcd(F_{k+1}, F_k) = 1$

So $P(k) \to P(k+1)$.

By Principle of Ind^n $P(n)$ true $\forall n \geq 2$.

Q4]... [20 points] You have access to a water faucet and two drinking glasses, one with capacity exactly 21oz and the other with capacity exactly 13oz. Is it possible to measure out exactly 1oz of water? Either describe a series of steps that ends up with 1oz, or prove that it is impossible.

$$\left.\begin{aligned} 21 &= 13(1) + 8 \\ 13 &= 8(1) + 5 \\ 8 &= 5(1) + 3 \\ 5 &= 3(1) + 2 \\ 3 &= 2(1) + 1 \\ 2 &= 1(2) + 0 \end{aligned}\right\} \Rightarrow \gcd(21,13) = 1.$$

Moreover

$$\begin{aligned} 1 &= 3 + 2(-1) = 3 + (5 + 3(-1))(-1) \\ &= 3(2) + 5(-1) \\ &= (8 + 5(-1))(2) + 5(-1) \\ &= 8(2) + 5(-3) \\ &= 8(2) + (13 + 8(-1))(-3) \\ &= 8(5) + 13(-3) \\ &= (21 + 13(-1))(5) + 13(-3) \\ &= 21(5) + 13(-8) \end{aligned}$$

Done!!

STRATEGY Fill 21 oz

Pour into 13 oz

→ empty 13 oz whenever full.

→ Refill 21 oz whenever empty.

After 5 fillings of 21 oz you'll eventually get to 1 oz!

	First Fill			2nd Fill				3rd Fill				4th Fill				5th Fill					
21 oz glass	21	8	8	∅	21	16	16	3	3	∅	21	11	11	∅	21	19	19	6	6	∅	21	14	14	1	1
13 oz glass	∅	13	∅	8	8	13	∅	13	∅	3	3	13	∅	11	11	13	∅	13	∅	6	6	13	∅	13	∅
			1st empty				2nd empty		3rd empty				4th empty				5th empty		6th empty		7th empty		8th empty	

You have access to a water faucet and two drinking glasses, one with capacity exactly 21oz and the other with capacity exactly 15oz. Is it possible to measure out exactly 1oz of water? Either describe a series of steps that ends up with 1oz, or prove that it is impossible.

$$\left.\begin{aligned} 21 &= 15(1) + 6 \\ 15 &= 6(2) + 3 \\ 6 &= 3(2) + 0 \end{aligned}\right\} \Rightarrow \gcd(21,15) = 3$$

$3 \mid 21$ & $3 \mid 15$ $\Rightarrow$ $3 \mid$ every integer linear combination of 21 & 15

But amount in a given glass at any stage is always an integer linear combination of 21 & 15.

$\Rightarrow$ $3 \mid$ amount in either glass at any stage

$\Rightarrow$ amount never equals 1 oz.

$\Rightarrow$ impossible!

Q5]. . . [20 points] Use modular exponentiation rules to compute the following powers in modular arithmetic.

1. $(23)^{50} \mod 17$

① → $23 \equiv 6 \mod 17$

② → $50 \equiv 2 \mod 16$

$(23)^{50} \equiv 6^{50} \equiv 6^2 \equiv 36 \equiv 2 \mod 17$.

(first $\equiv$: by ①; second $\equiv$: by Fermat & ②)

Answer. $2 \mod 17$

2. $(2016)^{2016} \mod 11$

① → $2016 \equiv 6 - 1 + 0 - 2 \equiv 3 \mod 11$ ← class notes on divisibility by 11.

② → $2016 \equiv 6 \mod 10$

$(2016)^{2016} \equiv 3^{2016} \equiv 3^6 \equiv (27)^2 \equiv 5^2 \equiv 3 \mod 11$.

(first $\equiv$: by ①; second $\equiv$: by Fermat & ②)

Answer. $3 \mod 11$

3. $3^{124} \mod 77$

$(7-1)(11-1) = (6)(10) = 60$

$124 \equiv 4 \mod 60$. ← ①

$3^{124} \equiv 3^4 \equiv 9^2 \equiv 81 \equiv 4 \mod 77$

($\equiv$: class notes on "mod pq" & ①)

Answer. $4 \mod 77$

Let p, q, r be three distinct prime numbers. Guess a **positive** integer power m so that

$$a^m \equiv 1 \mod pqr \qquad \text{for every integer } a \text{ such that } \gcd(a, pqr) = 1.$$

Now prove that your guess is correct.

Guess: $(p-1)(q-1)(r-1)$.

$\gcd(a, pqr) = 1 \Rightarrow \gcd(a,p) = 1$, $\gcd(a,q) = 1$ & $\gcd(a,r) = 1$.

Fermat ⇒ $a^{p-1} \equiv 1 \mod p$

$\Rightarrow a^{(p-1)(q-1)(r-1)} \equiv 1^{(q-1)(r-1)} \equiv 1 \mod p$

$\Rightarrow p \mid \left(a^{(p-1)(q-1)(r-1)} - 1\right)$

Fermat ⇒ $a^{q-1} \equiv 1 \mod q$

$\Rightarrow a^{(q-1)(p-1)(r-1)} \equiv 1^{(p-1)(r-1)} \equiv 1 \mod q$

$\Rightarrow q \mid \left(a^{(p-1)(q-1)(r-1)} - 1\right)$

Fermat ⇒ $a^{r-1} \equiv 1 \mod r$

$\Rightarrow a^{(p-1)(q-1)(r-1)} \equiv 1^{(p-1)(q-1)} \equiv 1 \mod r$

$\Rightarrow r \mid \left(a^{(p-1)(q-1)(r-1)} - 1\right)$

& p, q, r distinct primes

$\Rightarrow pqr \mid \left(a^{(p-1)(q-1)(r-1)} - 1\right) \Rightarrow a^{(p-1)(q-1)(r-1)} \equiv 1 \mod pqr$