Disc. Math! Mid II – Sol

Q1]... [25 points]

1. State the Principle of Induction.

$P(n)$ = statement involving natural number n.

$$\left.\begin{array}{l} \bullet\ P(1) \text{ true} \\ \bullet\ P(k) \text{ true} \Rightarrow P(k+1) \text{ true} \end{array}\right\} \Longrightarrow P(n) \text{ true } \forall n \in \mathbb{N}$$

2. Give a proof by induction of the following statement:

$$n! < n^n \qquad \forall n \in \mathbb{N}, n \geq 2.$$

Case $n=2$

$$2! = (2)(1) = 2 < 2^2 = 4$$

$$\boxed{2! < 2^2} \qquad P(2) \text{ true}$$

Inductive step

Suppose $P(k)$ true : $k! < k^k$

then
$$\begin{aligned} (k+1)! &= k!\,(k+1) \\ &< k^k\,(k+1) \quad \text{---- by } P(k) \text{ true (inductive hypothesis)} \\ &< (k+1)^k\,(k+1) \quad \text{---- since } k < (k+1) \Rightarrow k^k < (k+1)^k \\ &= (k+1)^{k+1} \end{aligned}$$

& so $P(k+1)$ follows.

By P. I., $P(n)$ true $\forall n \in \mathbb{N}$.

Q2]... [25 points]

1. State the Fundamental Theorem of Arithmetic.

Every integer > 1 can be expressed as a product of primes.

This expression is <u>unique</u> if the primes are written in non-decreasing order.

2. Use the Fundamental Theorem of Arithmetic to give a proof of the fact that $\sqrt{15}$ is irrational.

We argue by contradiction. Suppose $\sqrt{15} = p/q$ for some

$p, q \in \mathbb{N}$. Then

$$15 = p^2/q^2$$

$$\Rightarrow \quad (3)(5)q^2 = p^2 \quad \text{———} (*)$$

L.H.S. of $(*)$ is an integer (closure) and F.T.A. $\Rightarrow$

\# 3's in its prime decomposition $\equiv 1 \pmod 2$

(since \# 3's in prime decomp of $q^2 \equiv 0 \pmod 2$)

RHS of $(*)$ is the same integer and FTA $\Rightarrow$

\# 3's in its prime decomposition $\equiv 0 \pmod 2$.

This contradicts uniqueness in F.T.A.

$\Rightarrow$ original assumption that "$\sqrt{15} = p/q$ is rational" is false.

$\Rightarrow \sqrt{15}$ is irrational.

Q3]... [25 points]

1. Let m be a positive integer, and a, b be integers. Give the definition of the expression $a \equiv b \pmod{m}$.

$a \equiv b \pmod{m}$ means $m \mid (b-a)$

i.e. $(b-a) = mk$ for some $k \in \mathbb{Z}$.

2. Find the remainder on dividing 2014^{2014} by 7.

$2014 = (287)(7) + 5 \quad \Rightarrow \quad 2014 \equiv 5 \pmod{7} \equiv (-2) \pmod{7}$

$\Rightarrow (2014)^{2014} \equiv (-2)^{2014} \pmod{7}$

$\equiv (2)^{2014} \pmod{7}$ ... because 2014 is an <u>even</u> exponent.

$2^1 \equiv 2 \pmod{7}$
$2^2 \equiv 4 \pmod{7}$
$2^3 \equiv 1 \pmod{7} \leftarrow [8 \equiv 1 \bmod 7]$

$\Rightarrow 2^{2014} \equiv 2^{(3)(671)+1}$

$\equiv (2^3)^{671} \cdot 2$

$\equiv 1 \cdot 2$

$\equiv 2 \pmod{7}$ <u>Ans</u> $= \boxed{2}$

3. Without performing a division, test to see if 3141596 is divisible by 11. Show your work.

$3141596 = 6 + 9(10) + 5(10)^2 + 1(10)^3 + 4(10)^4 + 1(10)^5 + 3(10)^6$

$\equiv 6 + 9(-1) + 5(-1)^2 + 1(-1)^3 + 4(-1)^4 + 1(-1)^5 + 3(-1)^6 \pmod{11}$

$\equiv 6 - 9 + 5 - 1 + 4 - 1 + 3 \pmod{11}$

$\equiv 7 \pmod{11}$

$\Rightarrow$ 3141596 has a remainder of 7 on division by 11

$\Rightarrow$ is <u>not</u> divisible by 11.

Q4]. . . [25 points]

1. Give the definition of the greatest common divisor (a, b) of two integers a and b which are not both zero.

gcd (a,b) is the integer d satisfying:

(1) $d \mid a$ and $d \mid b$

(2) d is <u>largest</u> integer satisfying (1) above.

2. Use the Euclidean Algorithm to find the greatest common divisor of 21 and 44, and to find integers l and m such that

$$(21, 44) = 21l + 44m$$

$$\left.\begin{aligned} 44 &= 2(21) + 2 &&\Rightarrow (44,21) = (21,2) \\ 21 &= 10(2) + 1 &&\Rightarrow (21,2) = (2,1) \\ 2 &= 2(1) + 0 &&\Rightarrow (2,1) = 1 \end{aligned}\right\} \Rightarrow \gcd(44,21) = 1$$

back substitution...

$$\begin{aligned} 1 &= 21 - 10(2) \\ &= 21 - 10(44 - 2(21)) \\ &= 21 - 10(44) + 20(21) = 21(21) - 10(44) \end{aligned}$$

$$\boxed{\begin{aligned} m &= -10 \\ l &= 21 \end{aligned}}$$

3. Let a, b, c be integers. Prove that if $a \mid bc$ and $(a, b) = 1$, then $a \mid c$. State carefully any fact about (a, b) that you are using.

$$\left.\begin{aligned} (a,b) = 1 \Rightarrow \exists\, k, l \in \mathbb{Z} \text{ so that} \\ ka + lb = 1 \end{aligned}\right]$$

Key fact about (a,b).

(a,b) is integer linear combination of a & b.

Multiply across by c to get

$$\underbrace{kac}_{a \mid kac} + l\,\underbrace{bc}_{\text{told } a \mid bc} = c$$

$\Rightarrow a \mid (kac + lbc) \Rightarrow a \mid c$ done ☒