UBC MATH 312 MIDTERM REVIEW

SOLUTIONS TO 2 PROBLEMS FROM PROF. SUJATHA

(1) Since there are more multiples of 2 than 5 in $1, 2, 3, \ldots, n$, and $10 = 2 \times 5$, we see that the number of zeros at the end of $n!$ equals the number of 5's in the prime factorisation of $n!$. This is clearly an increasing function of n.

There are

$$\left[\frac{624}{5}\right] + \left[\frac{624}{5^2}\right] + \left[\frac{624}{5^3}\right]$$

$$= 124 + 24 + 4 = 152$$

zeros at the end of the decimal expansion of $624!$. However, since 5^4 divides 625, we see that there are $152 + 4 = 156$ zeroes at the end of the decimal expansion of $625!$. It follows that there cannot be 153, 154 or 155 zeroes at the end of the decimal expansion for any $n!$, $n \in \mathbb{N}$.

(2) Suppose $n!$ ends with exactly 74 zeroes.

Then $5^{74} \cdot 2^{74} = 10^{74}$ divides $n!$

As in question 1, since there are more multiples of 2 than 5 in $1, 2, 3, \ldots, n$, we need only concern ourselves with the fact that $5^{74} \mid n!$ Thus, we need to find an n such that $74 = \left[\frac{n}{5}\right] + \left[\frac{n}{5^2}\right] + \cdots$

By direct calculation, $74 = \left[\frac{300}{5}\right] + \left[\frac{300}{5^2}\right] + \left[\frac{300}{5^3}\right]$

It follows that $300!$, $301!$, $302!$, $303!$ and $304!$ end with exactly 74 zeroes in their decimal expansions.

UBC MATH 312 MIDTERM REVIEW

SOLUTIONS TO 8 SELECTED PROBLEMS FROM TEXTBOOK.

① [By induction.]

By assumption, $n \in \mathbb{N}$, $n \geq 5$.

Base Case. $n = 5$

$2^5 = 32 > 25 = 5^2$.

Induction Step.

Assume $2^k > k^2$ for some $k \in \mathbb{N}$, $k \geq 5$.

Then $2^{k+1} = 2 \cdot 2^k > 2 \cdot k^2 = k^2 + k^2$.

So it suffices to prove that $k^2 + k^2 \geq (k+1)^2$

$= k^2 + 2k + 1$.

So it suffices to prove that $k^2 \geq 2k + 1$

for $k \in \mathbb{N}$, $k \geq 5$.

But $k^2 \geq 2k + 1$

$\Updownarrow$

$k^2 - 2k - 1 \geq 0$

Let $f(x) = x^2 - 2x - 1 \in \mathbb{R}[x]$.

$f(5) = 5^2 - 2(5) - 1 = 14 > 0$

and $f'(x) = 2x - 2 > 0$ for all $x \geq 5$.

Thus, $2^{k+1} > (k+1)^2$.

Conclusion: By induction, $2^n > n^2$ for all $n \in \mathbb{N}$, $n \geq 4$.

(2) Let n be an <u>even</u> integer.

Then $n = 2k$ for some $k \in \mathbb{Z}$.

$$\begin{aligned} n - 2\left[\tfrac{n}{2}\right] &= 2k - 2\left[\tfrac{2k}{2}\right] \\ &= 2k - 2[k] \\ &= 2k - 2k \\ &= 0. \end{aligned}$$

Conversely,
Let n be an <u>odd</u> integer.

Then $n = 2k+1$ for some $k \in \mathbb{Z}$.

$$\begin{aligned} n - 2\left[\tfrac{n}{2}\right] &= (2k+1) - 2\left[\tfrac{2k+1}{2}\right] \\ &= 2k+1 - 2\left[k+\tfrac{1}{2}\right] \\ &= 2k+1 - 2k \\ &= 1 \neq 0. \end{aligned}$$

Since every integer $n \in \mathbb{Z}$ is either even or odd, we're done.

(3) In the section on Prime Numbers in the textbook, there is a theorem showing how to get n consecutive composite integers.

Following the proof of that theorem and letting $n = 1,000,000$, we get the consecutive composite integers

$$\left.\begin{array}{l} (1,000,001)! + 2, \\ (1,000,001)! + 3, \\ \vdots \\ (1,000,001)! + 1,000,001. \end{array}\right\} \text{one million integers}$$

as required. Note that for $2 \leq j \leq 1,000,001$, $j \mid (1,000,001)!$

(4) As $\gcd(a,b) = 1$, we can write

$$1 = ax + by \quad \text{for some } x, y \in \mathbb{Z}.$$

Similarly, as $\gcd(a,c) = 1$, we can write

$$1 = as + ct \quad \text{for some } s, t \in \mathbb{Z}.$$

Multiplying the 2 equations together gives

$$\begin{aligned} 1 = 1(1) &= (ax+by)(as+ct) \\ &= a(asx) + a(ctx) + a(bsy) + bc(ty) \\ &= a(asx + ctx + bsy) + bc(ty) \end{aligned}$$

Since $1 \in \mathbb{Z}$ can be expressed as a linear combination of a & bc, $\gcd(a, bc) \leq 1$

But since gcd of any 2 numbers in $\mathbb{Z}$ (not both zero) is at least 1, we have $\gcd(a, bc) = 1$

(5) $p \mid a^n = \underbrace{(a)(a)(a)\cdots(a)}_{n \text{ times}}$

section on Fundamental Theorem of Arithmet

By a theorem proven in the textbook, as p is prime, p has to divide at least one of the factors on the RHS.

But all of the factors on the RHS are "a."

So $p \mid a$.

(6) {This is a bit similar to one of the problems in the most recent homework, H/W #3}.

Case 1 $a = b = 1$

[Note: Unique prime factorisation only makes sense here for $ab \geq 2$]

Then $1 = ab = c^n$ for $c \in \mathbb{N}$ only makes sense for $c = 1$, in which case n can be any number $\in \mathbb{N}$

In this case, just let $d = e = 1 \in \mathbb{N}$.

Case 2 Either a or b is 1, but not both.

Without loss of generality, let $a = 1$, $b \neq 1$.

Then if we have $ab = c^n$, this implies

(1) $b = c^n \Rightarrow b = c^n$.

So in this case, just let $d = 1$ and $e = c$.

(6) (cont'd)

Case 3 $a, b \geq 2$.

$c^n = ab \geq 4 \implies c \neq 1$.

$\implies$ As $c \in \mathbb{N}$, $c \geq 2$.

Let $c = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ be the unique prime factorisation for c, where p_i are distinct p and $\alpha_i \in \mathbb{N}$.

Then $ab = c^n = p_1^{n\alpha_1} p_2^{n\alpha_2} \cdots p_r^{n\alpha_r}$.

But as $\gcd(a,b) = 1$, if a prime p_i appea in the prime factorisation of a, it cannot be in the prime factorisation of b (and vice versa

Thus, $a = \prod_{\substack{\text{some } i\text{'s} \\ \text{from } 1,2,\ldots,r}} p_i^{n\alpha_i}$ and $b = \prod_{\substack{\text{some } j\text{'s} \\ \text{from } 1,2,\ldots,r.}} p_j^{n\alpha_j}$

So let $d = \prod_{\substack{\text{same } i\text{'s} \\ \text{as in } a}} p_i^{\alpha_i}$ and $e = \prod_{\substack{\text{same } j\text{'s} \\ \text{as in } b.}} p_j^{\alpha_j}$

$\implies d, e \in \mathbb{N}$ and we have $a = d^n$ and $b =$

(7) As $2^{12} = 4096 \equiv 7 \pmod{47}$

and $7^2 = 49 \equiv 2 \pmod{47}$,

we can simply the quantity mod 47 as foll

$$2^{200} = 2^{192} \cdot 2^8$$

$$= (2^{12})^{16} \cdot 2^8$$

$$\equiv (7)^{16} \cdot 2^8 \pmod{47}$$

$$\equiv (7^2)^8 \cdot 2^8 \pmod{47}$$

$$\equiv 2^8 \cdot 2^8 \pmod{47}$$

$$\equiv 2^{12} \cdot 2^4 \pmod{47}$$

$$\equiv 7 \cdot 16 \pmod{47}$$

$$\equiv 112 \pmod{47}$$

$$\equiv 14 \pmod{47}$$

(8) We are given that $a\bar{a} \equiv 1 \pmod{m}$

and $b\bar{b} \equiv 1 \pmod{m}$.

Then $(ab)(\bar{a}\bar{b}) \equiv (a\bar{a})(b\bar{b}) \equiv 1 \cdot 1 = 1 \pmod{m}$.

Thus $\bar{a}\bar{b}$ is the inverse of $ab \pmod{m}$.