CSC165H1: Problem Set 2

Due Wednesday October 23 before 4 pm

1(a).

Let $n \in \mathbb{Z}$,

WTS: $9|n^2 \vee 3|n^2 - 1$

Let $q, r \in \mathbb{Z}$

$n = 3 \cdot q + r, 0 \leq r<3$ #Quotient Remainder Theorem

$r = 0$ or 1 or 2 #n is an integer

Case1: $r = 0, n = 3 \cdot q$

WTS: $9|n^2$ i.e., $\exists k_1 \in \mathbb{Z}, 9 \cdot k_1 = n^2$

Let: $k_1 = q^2$

$9 \cdot k_1 = 9 \cdot q^2$

$9 \cdot k_1 = (3 \cdot q)^2$

$9 \cdot k_1 = n^2$

Case2: $r = 1, n = 3 \cdot q + 1$

WTS: $3|n^2 - 1$ i.e., $\exists k_2 \in \mathbb{Z}, 3 \cdot k_2 = n^2 - 1$

Let: $k_2 = 3 \cdot q^2 + 2 \cdot q$

$3 \cdot k_2 = 9 \cdot q^2 + 6 \cdot q$

$3 \cdot k_2 = 9 \cdot q^2 + 6 \cdot q + 1 - 1$

$3 \cdot k_2 = (3 \cdot q + 1)^{2} - 1$

$3 \cdot k_2 = n^2 - 1$

Case3: $r = 2, n = 3 \cdot q - 2$

WTS: $3|n^2 - 1$ i.e., $\exists k_3 \in \mathbb{Z}, 3 \cdot k_3 = n^2 - 1$

Let: $k_3 = 3 \cdot q^2 - 4 \cdot q + 1$

$3 \cdot k_3 = 3 \cdot (3 \cdot q^2 - 4 \cdot q + 1)$

$3 \cdot k_3 = 9 \cdot q^2 - 12 \cdot q + 4 - 1$

$3 \cdot k_3 = (3 \cdot q - 2)^2 - 1$

$3 \cdot k_3 = n^2 - 1$ ■

1(b).

Prove by contradiction

Assume: the statement is false:

$\exists n \in \mathbb{Z}, \exists k \in \mathbb{Z}, 3k = n^2 - 2 \cdots\cdots$ 1

Since $\forall n \in \mathbb{N}, 9|n^2 \vee 3|n^2 - 1$ #Previous Problem, 1(a)

Case1: $3|n^2 - 1$

i.e., $\exists k_1 \in \mathbb{Z}, 3 \cdot k_1 = n^2 - 1$

$3 \cdot k = 3 \cdot k_1 - 1$ #1

$k = k_1 - \frac{1}{3}$

k is not an integer, contradiction!

Case2: $9|n^2$

i.e., $\exists k_2 \in \mathbb{Z}, 9 \cdot k_2 = n^2$

$3 \cdot k = 9 \cdot k_2 - 2$

$k = 3 \cdot k_2 - \frac{2}{3}$

k is not an integer, contradiction!

So, assumption is false, the original statement is true! ■

1(c).

$\forall n \in \mathbb{N}, n^2 \equiv 0 \pmod 4 \lor n^2 \equiv 1 \pmod 4$

Proof:

Case1: Let $n \in \mathbb{Z}$, n is even

i.e., $\exists k \in \mathbb{Z}, n = 2 \cdot k$

WTS: $n^2 \equiv 0 \pmod 4$

i.e., $\exists k_1 \in \mathbb{Z}, 4 \cdot k_1 = n^2$

Let $k_1 = k^2$

$4 \cdot k_1 = 4 \cdot k^2$

$4 \cdot k_1 = (2 \cdot k)^2$

$4 \cdot k_1 = n^2$

$n^2 \equiv 0 \pmod 4$

Case2: Let $n \in \mathbb{Z}$, n is odd

i.e., $\exists k' \mathbb{Z}, n = 2 \cdot k' + 1$

WTS: $n^2 \equiv 1 \pmod 4$

i.e., $\exists k_2 \in \mathbb{Z}, 4 \cdot k_2 = n^2 - 1$

Let $k_2 = k'^2 + k'$

$4 \cdot k_2 = 4 \cdot k'^2 + 4 \cdot k'$

$4 \cdot k_2 = (2 \cdot k' + 1)^2 - 1$

$4 \cdot k_2 = n^2 - 1$

$n^2 \equiv 1 \pmod 4$ ■

2(a).

Proof:

WTS: $\forall p_1, p_2, a, b \in \mathbb{Z}$, Prime(p1) $\wedge$ Prime(p2) $\wedge$ p1 $\neq$ p2 $\Longrightarrow$

$[a \equiv b \pmod{p_1 \cdot p_2} \Longrightarrow a \equiv b \pmod{p_1} \wedge a \equiv b \pmod{p_2}] \wedge$

$[a \equiv b \pmod{p_1} \wedge a \equiv b \pmod{p_2} \Longrightarrow a \equiv b \pmod{p_1 \cdot p_2}]$

Let $p_1, p_2, a, b \in \mathbb{Z}$

Proof of the first part:

Assume: $a \equiv b \pmod{p_1 \cdot p_2}$, Prime(p1) $\wedge$ Prime(p2) $\wedge$ p1 $\neq$ p2

i.e., $\exists k_1 \in \mathbb{Z}, p_1 \cdot p_2 \cdot k_1 = a - b$

WTS: $a \equiv b \cdot \pmod{p_1} \wedge a \equiv b \cdot \pmod{p_2}$

i.e., $\exists k_2, k_3 \in \mathbb{Z}, p_1 \cdot k_2 = a - b \wedge p_2 \cdot k_3 = a - b$

Let $k_2 = p_2 \cdot k_1, k_3 = p_1 \cdot k_1$

$p_1 \cdot k_2 = p_1 \cdot p_2 \cdot k_1 = a - b$ # $a \equiv b \pmod{p_1 \cdot p_2}$

$p_2 \cdot k_3 = p_1 \cdot p_2 \cdot k_1 = a - b$ # $a \equiv b \pmod{p_1 \cdot p_2}$

Proof of the second part:

Assume: $a \equiv b \pmod{p_1} \wedge a \equiv b \pmod{p_2}$, Prime(p1) $\wedge$ Prime(p2) $\wedge$ p1 $\neq$ p2

i.e., $\exists k_4, k_5 \in \mathbb{Z}, p_1 \cdot k_4 = a - b, p_2 \cdot k_5 = a - b$

WTS: $a \equiv b \pmod{p_1 \cdot p_2}$

i.e., $\exists k_6 \in \mathbb{Z}, p_1 \cdot p_2 \cdot k_6 = a - b$

Let $k_6 = \frac{k_4}{p_2}$ # k_4/p_2 is an integer:

$p_1 \cdot k_4 = a - b$

$p_2 \mid (a - b)$

$p_2 \mid p_1 \cdot k_4$

$p_2 \nmid p_1$ # p1 $\neq$ p2

so, $p_2 \mid k_4$

$p_1 \cdot p_2 \cdot k_6 = \frac{p_1 \cdot p_2 \cdot k_4}{p_2}$

$p_1 \cdot p_2 \cdot k_6 = p_1 \cdot k_4$

$p_1 \cdot p_2 \cdot k_6 = a - b$ #Assumption ■

2(b).

Proof:

First prove there exists x that satisfies the first two conditions:

$\forall$ a, b, p_1, $p_2 \in \mathbb{Z}$, $\exists x \in \mathbb{Z}$, Prime(p_1) $\wedge$Prime(p_2) $\wedge p_1 \neq p_2 \Longrightarrow$

$x \equiv a \pmod{p_1} \wedge x \equiv b \pmod{p_2}$

Let: a, b, p_1, $p_2 \in \mathbb{Z}$, $x \in \mathbb{Z}$

Assume: Prime(p_1) $\wedge$Prime(p_2) $\wedge p_1 \neq p_2$

WTS: $x \equiv a \pmod{p_1} \wedge x \equiv b \pmod{p_2}$

i.e., $\exists k_1 \in \mathbb{Z}, x - a = k_1 \cdot p_1$

$\exists k_2 \in \mathbb{Z}, x - b = k_2 \cdot p_2$

$\exists m_1, m_2 \in \mathbb{Z}, p_1 \cdot m_1 + p_2 \cdot m_2 = \gcd(p_1, p_2) = 1$ #Claim 6

$p_1 \cdot m_1 - 1 = - p_2 \cdot m_2$

$p_2 \cdot m_2 - 1 = - p_1 \cdot m_1$

Let: $x = b \cdot m_1 \cdot p_1 + a \cdot m_2 \cdot p_2$

Let: $k_2 = b \cdot (-m_2) + a \cdot m_2$

$p_2 \cdot k_2 = p_2\, b \cdot (-m_2) + p_2 \cdot a \cdot m_2$

$p_2 \cdot k_2 = b \cdot (m_1 \cdot p_1 - 1) + p_2 \cdot a \cdot m_2$

$p_1 \cdot m_1 - 1 = - p_2 \cdot m_2$

$p_2 \cdot k_2 = b \cdot m_1 \cdot p_1 + a \cdot m_2 \cdot p_2 - b$

$p_2 \cdot k_2 = x - b$

So, $x \equiv b \cdot \pmod{p_2}$

Let: $k_1 = a \cdot (-m_1) + b \cdot m_1$

$p_1 \cdot k_1 = p_1 \cdot a \cdot (-m_1) + p_1 \cdot b \cdot m_1$

$p_1 \cdot k_1 = a \cdot (m_2 \cdot p_2 - 1) + p_1 \cdot b \cdot m_1$

$p_2 \cdot m_2 - 1 = - p_1 \cdot m_1$

$p_1 \cdot k_1 = b \cdot m_1 \cdot p_1 + a \cdot m_2 \cdot p_2 - a$

$p_1 \cdot k_1 = x - a$

So, $x \equiv a \pmod{p_1}$

So, exists x that satisfies the first two conditions

Second proof there is only one x that $0 \leq x < p_1 \cdot p_2$:

For x' also satisfies the first two conditions, but $x' \neq x$

$x \equiv a \pmod{p_1}$ ……①

$x \equiv b \pmod{p_2}$ ……②

$x' \equiv a \pmod{p_1}$ ……③

$x, \equiv b \pmod{p_2}$ ……④

$x' - x \equiv 0 \pmod{p_1}$ #①, ③

$x' - x \equiv 0 \pmod{p_2}$ #②, ④

$x' - x \equiv 0 \pmod{p_1 \cdot p_2}$ #PS2 2(a)

$x' - x - 0 = k' \cdot p_1 \cdot p_2 \quad k' \in \mathbb{Z}$

$x' - x = k' \cdot p_1 \cdot p_2$

$x' \equiv x \pmod{p_1 \cdot p_2}$

$p_1 \cdot p_2 \mid x' - x$

for all X that satisfy the first two conditions:

$X = b \cdot m_1 \cdot p_1 + a \cdot m_2 \cdot p_2 + K \cdot p_1 \cdot p_2 \qquad K \in \mathbb{Z}$

if $K > 0$:

$X = b \cdot m_1 \cdot p_1 + a \cdot m_2 \cdot p_2 + K \cdot p_1 \cdot p_2$

$X > p_1 \cdot p_2$

Doesn't satisfy the last two conditions.

Only when $K = 0$:

$X = x = b \cdot m_1 \cdot p_1 + a \cdot m_2 \cdot p_2$

x satisfies all four conditions.

So, there is only one x that satisfies all four conditions. ■

3(a).

True.

Proof:

Let $e \in \mathbb{R}^{+}$,

Let $x \in \mathbb{R}$

Let $d = \frac{1}{8} \cdot e$

Assume: $|x| < d$

i.e., $|x| < \frac{1}{8} \cdot e$

WTS: $|7 \cdot x| < e$

$|7 \cdot x| = 7 \cdot |x|$

$|7 \cdot x| < 7 \cdot (\frac{1}{8} \cdot e)$

$|7 \cdot x| < \frac{7}{8} \cdot e$

$|7 \cdot x| < e$ ∎

3(b).

False

Negation: $\forall d \in \mathbb{R}^+, \exists e \in \mathbb{R}^+, \exists x \in \mathbb{R}, |\, x \,| < d \land |\, 7x \,| \geq e$

Proof:

Let: $d \in \mathbb{R}^+$

Let: $x = d/2$

Let $e = d$

WTS: $|x| < d \land |7x| \geq e$

$|x| = x$ # $x = d/2, d > 0$

$|x| = d/2$

$|x| < d$

$|7 \cdot x| = 7 \cdot |x|$

$|7 \cdot x| = 7 \cdot x$ # $x = d/2, d > 0$

$|7 \cdot x| = (\frac{7}{2}) \cdot d$

$|7 \cdot x| \geq d$

$|7 \cdot x| \geq e$ #$e = d$ ■

3(c).

True.

Proof:

Let: $d \in \mathbb{R}^+$

Let: $x \in \mathbb{R}$

Let: $e = 7 \cdot d$

Assume: $|x| < d$

WTS: $|7 \cdot x| < e$

$|7 \cdot x| = 7 \cdot |x|$

$|7 \cdot x| < 7 \cdot d$ #Assumption

$|7 \cdot x| < e$ # $e = 7 \cdot d$ ■

4(a).

Proof by contradiction:

Assumption1: If the statement is false.

Let $k \in \mathbb{Z}$, there are k primes congruent to 5 (mod 6)

S: $\{P_1, P_2, \cdots, P_k\}$

Let: $M = 6\times P_1\times P_2\times\cdots\times P_k - 1$

$M = 6\times P_1\times P_2\times\cdots P_k + 6 - 5$

$M = 6\times(P_1\times P_2\times\cdots P_k+1) - 5$

So: $M \equiv 5 \pmod 6$

Case 1: M is a prime

$M \equiv 5 \pmod 6$

M is not in S

Contradiction!

Case 2: M is not a prime

Let n be a prime, such that $n|M \wedge n \equiv 5 \pmod 6$ #Additional Proof

Additional Proof:

WTS: $\forall M\in\mathbb{N}, \exists n \in \mathbb{N}, \neg Prime(M) \wedge M \equiv 5 \pmod 6 \Rightarrow Prime(n) \wedge n|M \wedge n\equiv 5 \pmod 6$

First prove: $\forall n\in \mathbb{N}, Prime(n) \Rightarrow n=2 \vee n=3 \vee n \equiv 5 \pmod 6 \vee n \equiv 1 \pmod 6$

$n = 6d + r$ $(0\leq r<6)$ *#Quotient Remainder Theorem*

Case 1 $d = 0$:

Case 1.1: $r = 0, n = 0$ $\neg Prime(n)$

Case 1.2: $r = 1, n = 1$ $\neg Prime(n)$

Case 1.3: $r = 2, n = 2$ $Prime(n)$

Case 1.4: $r = 3, n = 3$ $Prime(n)$

Case 1.5: $r = 4, n = 4$ $\neg Prime(n)$

Case 1.6: $r = 5, n = 5$ $Prime(n)$ $n\equiv 5 \pmod 6$

Case 2 $d > 0$:

Case 2.1: $r = 0$ $6|n$ $\neg Prime(n)$

Case 2.2: $r = 1$ $n \equiv 1 \pmod 6$, *may be prime, like 7*

Case 2.3: $r = 2$ $2|n$ $\neg Prime(n)$

Case 2.4: $r = 3$ $3|n$ $\neg Prime(n)$

Case 2.5: $r = 4$ $\quad 2|n \qquad \neg Prime(n)$

Case 2.6: $r = 5$ $\quad n \equiv 5 (\bmod 6)$ may be prime like 11

We proved $\forall n \in \mathbb{N}, Prime(n) \Longrightarrow n=2 \vee n=3 \vee n \equiv 5 \ (\bmod 6) \vee n \equiv 1 (\bmod 6)$

Next prove the original statement:

Let $M \in \mathbb{N}$

Assume: $\neg Prime(M) \wedge M \equiv 5 \ (\bmod 6)$

WTS: $\exists n \in \mathbb{N}, Prime(n) \wedge n|M \wedge n \equiv 5 \ (\bmod 6)$

Since $\neg Prime(M)$

then M can be written as multiplication of many primes

Since $M \equiv 5 \ (\bmod 6)$ so $M \neq 0, M \neq 1$

$M = P_1 \times P_2 \times \cdots P_m$

Prove by contradiction: Assumption 2: if no P_i satisfies $P_i \equiv 5 \ (\bmod 6)$,

Let $m_1, m_2, m \in \mathbb{N}$

Case 1: $M = 2^m$:

$\forall k_1 \in \mathbb{Z}, 2^m - 5 \neq 6k$ $\qquad$ # $2^m - 5$ is odd, $6k$ is even

$M \not\equiv 5 \ (\bmod 6)$, Contradiction!

Case 2: $M = 3^{m,}$

$\forall k_2 \in \mathbb{Z}, 3^m - 5 \neq 6k$ $\qquad$ # otherwise $k = \frac{3^{m-1}}{2} - \frac{5}{6}$, not integer

$M \not\equiv 5 (\bmod 6)$, Contradiction!

Case 3: $M = 2^{m1} \cdot 3^{m2}$:

$\forall k_3 \in \mathbb{Z}, 2^{m1} \cdot 3^{m2} - 5 \neq 6k$ $\quad$ # otherwise $k = 2^{m-1} \cdot 3^{m-1} - \frac{5}{6}$ not Integer

$M \not\equiv 5 \ (\bmod 6)$, Contradiction!

Case 4: $M = (6d_1 + 1) \cdot (6d_2 + 1) \cdots (6d_m + 1) \cdot 2^{m1} \cdot \ 3^{m2}$

Case 4.1: $m_1 = m_2 = 0$

$M = (6d_1 + 1) \cdot (6d_2 + 1) \cdots (6d_m + 1) = 6D + 1$

$\forall k_4 \in \mathbb{Z}, 6D + 1 - 5 \neq 6K$ #Otherwise $k = D - 4/6$ is not integer

$M \not\equiv 5 \ (\bmod 6)$, Contradiction!

Case 4.2: $m_1 \neq 0$,

$M = (6d_1 + 1) \cdot (6d_2 + 1) \cdots (6d_m + 1) \cdot 2^{m1} \cdot 3^{m2}$

$\forall k_5 \in \mathbb{Z}, M - 5 \neq 6k$ # m-5 is odd, 6k is even

$M \not\equiv 5 \pmod 6$, Contradiction!

Case 4.3: $m_1 = 0, m_2 \neq 0$

$M = (6d_1 + 1)(6d_2 + 1) \cdots (6d_m + 1) \cdot 3^{m2} 3^{m2}$

$= (6D + 1)\, 3^{m2}$

$\forall k_6 \in \mathbb{Z}, M - 5 \neq 6k$ #Otherwise $k = D \cdot 3^{m2} + 3^{m2-1}/2$ not integer

$M \not\equiv 5 \pmod 6$, Contradiction!

So, Assumption 2 is False, we have proved the additional proof

If $n \in S$:

$n|M \wedge n|M-1$ then $n|1$, contradiction #n is a prime, no prime divides 1

If $n \notin S$: contradiction!

So, Assumption1 is False, there are infinite primes congruent to 5(mod6) ■

4(b).

$\forall n \in \mathbb{N}, \exists m \in \mathbb{N}, \neg\text{Prime}(m) \wedge m > n \wedge m \equiv 5 \pmod 6$

Proof:

Let $n \in \mathbb{N}$, $k' = n+1$, $k = 5k'$

Let $m = 6k + 5$

$m = 6 \times 5 \times k' + 5$

$m = 6 \times 5 \times (n+1) + 5$

$m = 30n + 35$

$m > n$

$m-5 = 6k$

$m \equiv 5 \pmod 6$

$m = 5(6k' + 1)$ # $k = 5k'$

m is not a prime ■

5.

P(n): Every sets of size n has $\frac{n(n-1)(n-2)(n-3)}{24}$ subsets of size 4

Proof:

Base case:

P(0): all sets of size 0 have 0 subsets of size 4

$\frac{0(0-1)(0-2)(0-3)}{24} = 0$, verified

Induction step:

Induction hypothesis: P(n): $n \geq 0$, all sets with size n have $\frac{n(n-1)(n-2)(n-3)}{24}$ subsets of size 4

P(n+1):

WTS: All sets with size n+1: $\{e_1, e_2, \cdots e_n\} \cup \{e_{n+1}\}$ has $\frac{(n+1)\cdot n \cdot (n-1)\cdot(n-2)}{24}$ subsets of size 4

All subsets without $\{e_{n+1}\}$: $\frac{n(n-1)(n-2)(n-3)}{24}$

#Induction hypothesis

All subsets with $\{e_{n+1}\}$: $\frac{n(n-1)(n-2)}{6}$ #problem header

Total: $\frac{n(n-1)(n-2)(n-3)}{24} + \frac{n(n-1)(n-2)}{6}$

$= \frac{(n-1)(n-2)[4n+n(n-3)]}{24}$

$= \frac{(n+1)\cdot n \cdot (n-1)\cdot(n-2)}{24}$ ■

6.

P(0): $n = m = 0$, $P = 0$, $b_0 = 0$, $0 = \sum_{i=0}^{p} b_i \cdot 2^i = 0 \times 2^0 = 0$

P(1): $n = m = 1$, n is odd

$\exists\, k \in \mathbb{N}, n = 2k + 1, k = 0$

$P = 0, k = \sum_{i=0}^{p} b_i \cdot 2^i = 0$

$n = 2(\sum_{i=0}^{p} b_i \cdot 2^i) + 1 = (\sum_{i=0}^{p} b_i 2^{i+1}) + 1$

$P' = P + 1$, $b_0' = 1$ for all $i \in \{0, 1\}$, let $b_i' = b_{i-1}$

Then $1 = \sum_{i=0}^{p'} b_i' 2^i = 01$

P(2): $n = m = 2$, n is even

$\exists\, k \in \mathbb{N}, n = 2k, k = 1$

$P = 1, k = \sum_{i=0}^{p} b_i \cdot 2^i = 01$

$P' = P + 1 = 2$, $b_0' = 0$, for all $i \in \{0, 1, 2\}$, $b_i' = n_{i-1}$

Then $n = \sum_{i=0}^{p'} b_i' \cdot 2^i = 010$

P(3): $n = m = 3$, n is odd

$\exists k \in \mathbb{N}, n = 2k+1, k = 1$

$P = 1, k = \sum_{i=0}^{p} b_i 2^i = 01$

$P' = P + 1 = 2$, $b_0' = 1$, for all $i \in \{0, 1, 2\}$, $b_i' = b_{i-1}$

Then $n = \sum_{i=0}^{p'} b_i' 2^i = 011$

P(4): $n = m =4$, n is even

$\exists\, k \in \mathbb{N}, n = 2k, k = 2$

$P = 2, k = \sum_{i=0}^{p} b_i \cdot 2^i = 010$

$P' = P+1 = 3$, $b_0 = 0$, for all $i \in \{0, 1, 2, 3\}$, $b_i' = b_i - 1$

Then $n = \sum_{i=0}^{p'} b_i' \cdot 2^i = 0100$

P(5): $n = m = 5$, n is odd

$\exists\, k \in \mathbb{N}, n = 2k+1, k = 2$

$P = 2, k = \sum_{i=0}^{p} b_i \cdot 2^i = 010$

$P' = P+1 = 3$, $b_0 = 1$, for all $i \in \{0, 1, 2, 3\}$, $b_i = b_i - 1$

Then $n = \sum_{i=0}^{p'} b_i' \cdot 2^i = 0101$

5 is 0101, The reason there is a zero at the left most digit is that the algorithm makes 1 to 01, so there will always be a 0 at the left most digit. ■