CSC165H1 Problem Set 2

Xiaoyu Zhou, Yichen Xu

February 10, 2019

1. Difference of Squares

   (a) $\forall n \in \mathbb{Z}^+$, DifferenceOfSquare(n) $\Rightarrow (\exists k_1 \in \mathbb{Z}, n = 2k_1 - 1) \vee (\exists k_2 \in \mathbb{Z}, n = 4k_2)$

   (b) *Proof*
   Let $n \in \mathbb{Z}$. Assume that there exits $p, q \in \mathbb{Z}$, $n = p^2 - q^2$.
   Let's divide the proof into four cases.

      i. Both p and q are odd.
      Thus, $\exists k_1, k_2 \in \mathbb{Z}, p = 2k_1 + 1, q = 2k_2 + 1$. Let $k_3 = k_1^2 + k_1 - k_2^2 - k_2$
      $n = p^2 - q^2$
      $n = (2k_1 + 1)^2 - (2k_2 + 1)^2$
      $n = 4k_1^2 + 4k_1 + 1 - 4k_2^2 - 4k_2 - 1$
      $n = 4k_1^2 + 4k_1 - 4k_2^2 - 4k_2$
      $n = 4(k_1^2 + k_1 - k_2^2 - k_2)$
      $n = 4k_3$
      So, n can be divided by 4.

      ii. Both p and q are even.
      Thus, $\exists k_1, k_2 \in \mathbb{Z}, p = 2k_1, q = 2k_2$. Let $k_3 = k_1^2 - k_2^2$
      $n = p^2 - q^2$
      $n = (2k_1)^2 - (2k_2)^2$
      $n = 4k_1^2 - 4k_2^2$
      $n = 4(k_1^2 - k_2^2)$
      $n = 4k_3$
      So, n can be divided by 4.

      iii. p is even, q is odd.
      Thus, $\exists k_1, k_2 \in \mathbb{Z}, p = 2k_1, q = 2k_2 + 1$. Let $k_3 = 2k_1^2 - 2k_2^2 - 2k_2 - 1$
      $n = p^2 - q^2$
      $n = (2k_1)^2 - (2k_2 + 1)^2$
      $n = 4k_1^2 - 4k_2^2 - 4k_2 - 1$
      $n = 4k_1^2 - 4k_2^2 - 4k_2 - 2 + 1$
      $n = 2(2k_1^2 - 2k_2^2 - 2k_2 - 1) + 1$
      $n = 2k_3 + 1$
      So, n is an odd number.

iv. p is odd, q is even.
Thus, $\exists k_1, k_2 \in \mathbb{Z}, p = 2k_1 + 1, q = 2k_2$. Let $k_3 = 2k_1^2 + 2k_1 - 2k_2^2$
$n = p^2 - q^2$
$n = (2k_1 + 1)^2 - (2k_2)^2$
$n = 4k_1^2 + 4k_1 + 1 - 4k_2^2$
$n = 2(2k_1^2 + 2k_1 - 2k_2^2) + 1$
$n = 2k_3 + 1$
So, n is an odd number.

(c) *Negation:* $\exists x, y \in \mathbb{Z}^+$, DifferenceOfSquares(x) $\wedge$ DifferenceOfSquares(y) $\wedge\neg$ DifferenceOfSquares(x + y)
Proof
Let $x = 3, y = 7$.
There exist $p_1 = 2, p_2 = 4, q_1 = 1, q_2 = 3$ to make $x = p_1^2 - q_1^2, y = p_2^2 - q_2^2$. Thus, x, y are difference of squares.
From question a. we can know that every difference of squares is odd or divisible by four.
However, $x + y = 3 + 7 = 10$, is neither odd nor divisible by four. So, 10 is not a difference of squares.

2. Greatest common divisor and divisibility.

(a) *Translation.* $\forall a, m, n \in \mathbb{Z}$, gcd(m, n) = gcd(n, $m - an$)
Proof.
Let $a, m, n \in \mathbb{Z}$. Let $x = gcd(m, n)$, $y = gcd(n, m - an)$. That means that $x|m$, $x|n$, $y|n$, $y|(m - an)$. Let's divide the proof into three parts.

i. Proof $x \leq y$
By using fact 2, we can know that $x|(m - an)$.
From the definition of the greatest common divisor, we can know that $x \leq y$.

ii. Proof $y \leq x$
Since $m = m - an + an$ and fact 2, $y|m$.
From the definition of the greatest common divisor, we can know that $y \leq x$.

iii. Proof $x = y$
Because $x \leq y$ and $y \leq x$, $x = y$, which means that $gcd(m, n) = gcd(n, m-an)$

(b) *Negation:* $\exists a, m, n \in \mathbb{Z}$, gcd(m, n) $\neq$ gcd(n, $m - an$)
Proof.
Let $m = 8, n = 2, a = 2$.
Then gcd(m, n) = gcd(8, 2) = 2
gcd$(m, m - an)$ = gcd(8, 4) = 4
Since $2 \neq 4$, gcd(m, n) $\neq$gcd$(m, m - an)$

(c) *Translation.* $\forall m, n \in \mathbb{Z}, (\exists k \in \mathbb{Z}, m = 2k - 1) \Rightarrow gcd(m, n) = gcd(m, 2n)$

Proof.

Let $m, n \in \mathbb{Z}$. Assume m is odd, which means that $\exists k \in \mathbb{Z}, m = 2k - 1$. Let a = gcd(m,n), b = gcd(m, 2n). That means that $a|m$, $a|n$, $b|m$, $b|2n$. Let $2n = b * c$ where c is an integer. Let's divide the proof into three parts.

i. Proof $b \leq a$

By using the contrapositive of fact 1, we can know that $\neg 2|m \Rightarrow \neg 2|b \vee \neg b|m$. Since m is odd, so 2 cannot divide m. Moreover, $b|m$. Thus, 2 cannot divide b.

By using the contrapositive of fact 3, we can know that $2|2n \Rightarrow 2|c \vee 2|b$. Since 2 cannot divide b, $2|c$. Thus $\frac{c}{2}$ is an integer.

$n = b * \frac{c}{2}$, where b, $\frac{c}{2}$ are all integers. That means that $b|n$.

Because of the definition of the greatest common divisor, $b \leq a$.

ii. Proof $a \leq b$

Since $a|n$, $b|2n$.

Because of the definition of the greatest common divisor, $a \leq b$.

iii. Proof $a = b$

Because $a \leq b$ and $b \leq a$, $a = b$, which means that $gcd(m, n) = gcd(m, 2n)$

(d) *Translation.*$\forall n \in \mathbb{N}, gcd(n^2 + n + 1, (n + 1)^2 + (n + 1) + 1) = 1$

Proof.

Let $n \in \mathbb{N}, p = n^2$, $q = n + 1$

$n^2 + n + 1 = p + q$

$(n + 1)^2 + (n + 1) + 1 = n^2 + 3n + 3 = p + 3q$

Thus, $gcd(n^2 + n + 1, (n + 1)^2 + (n + 1) + 1) = gcd(p + q, p + 3q)$.

As we proven: $\forall a, m, n \in \mathbb{Z}, gcd(m, n) = gcd(n, m - an)$, $gcd(p + q, p + 3q) = gcd(p + 3q, 2q) = gcd(n^2 + 3n + 3, 2n + 2)$

$2n + 2$ can only divided by $2n + 2$, $n + 1$, 2 and 1. However, $n^2 + 3n + 3$ cannot divided by $2n + 2$, $n + 1$ or 2. Thus, 1 is the only common divisor of $n^2 + 3n + 3$ and $2n + 2$, which means that $gcd(n^2 + n + 1, (n + 1)^2 + (n + 1) + 1) = 1$

3. Eventually bounded.

(a) *Translation:* $\exists n_0 \in \mathbb{N}, \exists y \in \mathbb{R}^{\geq 0}, \forall n \in \mathbb{N}, n \geq n_0 \Rightarrow \frac{1}{n+1} \leq y$

Proof

Let $n_0 = 1, y = \frac{1}{2}$.

$\frac{1}{n+1} \leq \frac{1}{n_0+1}$ (since $n \geq n_0$)

$= \frac{1}{1+1}$

$= \frac{1}{2}$

Thus, $\frac{1}{n+1} \leq \frac{1}{2}$

(b) *Proof*

Let $f : \mathbb{N} \rightarrow \mathbb{R}^{\geq 0}$ be a function. Assume that $\forall x, y \in \mathbb{R}, x > y \Rightarrow f(x) < f(y)$.

We want to prove $\exists a \in \mathbb{N}, \exists b \in \mathbb{R}^{\geq 0}, \forall n \in \mathbb{N}, n \geq a \Rightarrow f(n) \leq b$.
Let $a = 1, n \in \mathbb{N}$ and $n \geq a$. Let $b = f(a)$.
Because of the assumption and $n \geq a$, $f(n) \leq f(a) = b$
Thus, $\exists a \in \mathbb{N}, \exists b \in \mathbb{R}^{\geq 0}, \forall n \in \mathbb{N}, n \geq a \Rightarrow f(n) \leq b$.

(c) *Proof*
Let $f_1 : \mathbb{N} \to \mathbb{R}^{\geq 0}$ and $f_2 : \mathbb{N} \to \mathbb{R}^{\geq 0}$ be functions. Assume f_1 and f_2 are eventually founded, which means: $(\exists a_1 \in \mathbb{N}, \exists b_1 \in \mathbb{R}^{\geq 0}, \forall n_1 \in \mathbb{N}, n_1 \geq a_1 \Rightarrow f_1(n_1) \leq b_1)$, $(\exists a_2 \in \mathbb{N}, \exists b_2 \in \mathbb{R}^{\geq 0}, \forall n_2 \in \mathbb{N}, n_2 \geq a_2 \Rightarrow f_2(n_2) \leq b_2)$. We want to prove $\exists a_3 \in \mathbb{N}, \exists b_3 \in \mathbb{R}^{\geq 0}, \forall n_3 \in \mathbb{N}, n_3 \geq a_3 \Rightarrow (f_1 \times f_2)(n_3) \leq b_2$.
Let $a_3 = a_1 + a_2$. Let $b_3 = b_1 * b_2$. Let $n_3 \in \mathbb{N}$, assume $n_3 \geq a_3$.
From the previous assumptions, since $n_3 \geq a_3 \geq a_1$, $f_1(n_3) \leq b_1$. Since $n_3 \geq a_3 \geq a_2$, $f_2(n_3) \leq b_2$.
$(f_1 \times f_2)(n_3)$
$= f_1(n_3) * f_2(n_3)$
$\leq b_1 * b_2$ (since b_1, b_2 all larger than 0) $= b_3$
Thus, $\exists a_3 \in \mathbb{N}, \exists b_3 \in \mathbb{R}^{\geq 0}, \forall n_3 \in \mathbb{N}, n_3 \geq a_3 \Rightarrow (f_1 \times f_2)(n_3) \leq b_2$