CSC165H1: Problem Set2

Pan Chen, Yang Shang, Dejun Yang

February 10, 2019

1 Difference of Squares

(a)

$$\forall n \in \mathbb{Z}^+, DifferenceOfSquares(n) \Rightarrow (\exists k \in \mathbb{Z}^+, n = 2k - 1 \vee n = 4k) \quad (1)$$

(b)

Proof. $\forall n \in \mathbb{Z}^+$. Assume DifferenceOfSquares(n), i.e, $\exists p, q \in \mathbb{Z}^+, n = p^2 - q^2$.

Because we know $n, p, q \in \mathbb{Z}^+$, we can conclude:

$n = p^2 - q^2 > 0$

$p^2 > q^2$

$p > q$ (Because $p, q \in \mathbb{Z}^+$)

By the Quotient-Remainder Theorem, we get the conclusion that when p, q are divided by 2, the only two possible remainders are 0 and 1.

Therefore, we will divide up the proof into four cases based on these remainders.

Case 1: Assume the remainder when p, q are divided by 2 are both 0. That is, we assume $\exists k_1, k_2 \in \mathbb{Z}^+$ such that $p = 2k_1, q = 2k_2$. By the previous deduction that $p > q$, we know $k_1 > k_2$ We want to prove $4|n$, i.e, $\exists k \in \mathbb{Z}^+, n = 4k$.

Let $k = k_1^2 - k_2^2$.

We have:

$$n = p^2 - q^2$$

$$n = (2k_1)^2 - (2k_2)^2$$

$$n = 4k_1^2 - 4k_2^2$$

$$n = 4(k_1^2 - k_2^2)$$

$$n = 4k$$

Therefore, we know that in this case, $4|x$ is True, so the whole statement is True in this case.

Case 2: Assume the remainder when p, q are divided by 2 are 0 and 1 respectively. That is, we assume $\exists k_1, k_2 \in \mathbb{Z}^+$ such that $p = 2k_1, q = 2k_2 - 1$. By the previous deduction that $p > q$, we know $2k_1 > 2k_2 - 1$.

So, we have:

$(2k_1)^2 > (2k_2 - 1)^2$

$4k_1^2 > 4k_2^2 - 4k_2 + 1$

$4(k_1^2 - k_2^2 + k_2) > 1$

$2k_1^2 - 2k_2^2 + 2k_2 > \frac{1}{2}$

And because $k_1, k_2 \in \mathbb{Z}^+$, so $(2k_1^2 - 2k_2^2 + 2k_2) \in \mathbb{Z}^+$

In this case, we want to prove $\exists k \in \mathbb{Z}^+, n = 2k - 1$.

Let $k = 2k_1^2 - 2k_2^2 + 2_k^2$.

We have:

$$n = p^2 - q^2$$

$$n = (2k_1)^2 - (2k_2 - 1)^2$$

$$n = 4k_1^2 - 4k_2^2 + 4k_2 - 1$$

$$n = 2(k_1^2 - k_2^2 + 2k_2) - 1$$

$$n = 2k - 1$$

Therefore, we know that in this case, $\exists k \in \mathbb{Z}^+, n = 2k - 1$ is True, so the whole statement is True in this case.

Case 3: Assume the remainder when p, q are divided by 2 are 1 and 0 respectively. That is, we assume $\exists k_1, k_2 \in \mathbb{Z}^+$ such that $p = 2k_1 - 1, q = 2k_2$. By the previous deduction that $p > q$, we know $2k_1 - 1 > 2k_2$.

So, we have:

$(2k_1 - 1)^2 > (2k_2)^2$

$4k_1^2 - 4k_1 + 1 > 4k_2^2$

$4k_1^2 - 4k_1 - 4k_2^2 + 2 - 1 > 0$

$2(2k_1^2 - 2k_1 - 2k_2^2 + 1) > 1$

$(2k_1^2 - 2k_1 - 2k_2^2 + 1) > \frac{1}{2}$

And because $k_1, k_2 \in \mathbb{Z}^+$, so $(2k_1^2 - 2k_1 - 2k_2^2 + 1) \in \mathbb{Z}^+$.

In this case, we want to prove $\exists k \in \mathbb{Z}^+, n = 2k - 1$.

Let $k = 2k_1^2 - 2k_1 - 2k_2^2 + 1$.

We have:

$$n = p^2 - q^2$$

$$n = (2k_1 - 1)^2 - (2k_2)^2$$

$$n = 4k_1^2 - 4k_1 + 1 - 4k_2^2$$

$$n = 2(2k_1^2 - 2k_1 - 2k_2^2 + 1) - 1$$

$$n = 2k - 1$$

Therefore, we know that in this case, $\exists k \in \mathbb{Z}^+, n = 2k - 1$ is True, so the whole statement is True in this case.

Case 4: Assume the remainder when p, q are divided by 2 are both 1. That is, we assume $\exists k_1, k_2 \in \mathbb{Z}^+$ such that $p = 2k_1 - 1, q = 2k_2 - 1$. By the previous deduction that $p > q$, we know $2k_1 - 1 > 2k_2 - 1$, so $k_1 > k_2$.

So, we have:

And since $k_1, k_2 \in \mathbb{Z}^+$, we know $k_1 + k_2 - 1 > 0$.

Therefore, we have:

$2(k_1 + k_2 - 1)(k_1 - k_2) > 0$

$2k_1^2 - 2k_2^2 - 2k_1 + 2k_2 > 0$

$k_1^2 - k_2^2 - k_1 + k_2 > 0$

And because $k_1, k_2 \in \mathbb{Z}^+$, so $k_1^2 - k_2^2 - k_1 + k_2 \in \mathbb{Z}^+$.

And in this case, we want to prove $\exists k \in \mathbb{Z}^+, n = 4k$.

Let $k = k_1^2 - k_2^2 - k_1 + k_2$.

We have:

$$n = p^2 - q^2$$

$$n = (2k_1 - 1)^2 - (2k_2 - 1)^2$$

$$n = (4k_1^2 - 4k_1 + 1) - (4k_2^2 - 4k_2 + 1)$$

$$n = 4k_1^2 - 4k_2^2 - 4k_1 + 4k_2$$

$$n = 4(k_1^2 - k_2^2 - k_1 + k_2)$$

$$n = 4k$$

Therefore, we know that in this case, $\exists k \in \mathbb{Z}^+, n = 4k$ is True, so the whole statement is True in this case.

So, $\forall n \in \mathbb{Z}^+$. Assume DifferenceOfSquares(n), i.e, $\exists p, q \in \mathbb{Z}^+, n = p^2 - q^2$ □

(c)

Proof. We will disprove this statement. In other words, we will prove the negation.

Negation: $\exists x, y \in Z^+, DifferenceOfSquares(x) \wedge DifferenceOfSquares(y) \wedge \neg DifferenceOfSquares(x + y)$

Let x = 3, y = 3. Then, DifferenceOfSquares(x) because $x = 3 = 2^2 - 1^2$ and DifferenceOfSquares(y) because $y = 3 = 2^2 - 1^2$

And x + y = 6.

The contrapositive of statement from part(a) is:

$\forall n \in \mathbb{Z}^+, \forall k \in \mathbb{Z}^+, n \neq 2k-1 \wedge n \neq 4k \Rightarrow \neg DifferenceOfSquares(n)$

And because 6 / 4 = 1.5 and $1.5 \notin \mathbb{Z}^+$, so there is not $k \in \mathbb{Z}^+$ such that $n = 4k$,

i.e, $\forall k \in \mathbb{Z}^+, n \neq 4k$.

And because 6 is an even number, which means 6 is not an odd number, so

$\forall k \in \mathbb{Z}^+, n \neq 2k-1$.

Therefore, $\forall n \in \mathbb{Z}^+, \forall k \in \mathbb{Z}^+, n \neq 2k-1 \wedge n \neq 4k)$, so $\neg DifferenceOfSquares(x+y)$.

So, $\exists x, y \in Z^+, DifferenceOfSquares(x) \wedge DifferenceOfSquares(y) \wedge \neg DifferenceOfSquares(x+y)$

So, the negation is True. Therefore, the original statement is False. ☐

2 Greatest Common divisor and divisibility

(a)

Proof. We want to prove: $\forall m, n \in \mathbb{Z}, gcd(m, n) = gcd(n, m - an)$.

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

We will divide our proof into two cases, depending on whether m, n are both 0 or not.

Case 1: Assume m = n = 0

Then gcd(m, n) = gcd(0, 0)

gcd(n, m - an) = gcd(0, 0)

Hence, gcd(m, n) = gcd(n, m- an)

Case 2: Assume that m, n are not all zero.

Because $1|m, 1|n, 1|(m-an)$, so m and n at least have a common divisor 1, n and (m - an) at least have a common divisor 1.

So, assume x = gcd(m, n), y = gcd(n, m - an).

Hence, all we want to show is that x = y, i.e, $x \leq y$ and $y \leq x$.

Since x = gcd(m, n), $x|m$ and $x|n$.

From fact 2 we know that $x|(1 \times m + (-a) \times n)$

That is, $x|m - an$.

And we know $x|n$, so x is also a common divisor of n and m-an. So from the definition of greatest common divior, since y = gcd(n, m - an), we have $x \leq y$.

And since y = gcd(n, m - an), so $y|n$ and $y|m - an$. So $\exists k_1, k_2 \in \mathbb{Z}, n = k_1 y, m - an = k_2 y$

Want to show $y|m$, i.e, $\exists k \in Z, m = ky$

Let $k = ak_1 + k_2$.

Because $n = k_1 y, m - an = k_2 y$, by substituting n in the second equation, we get:

$m - ak_1 y = k_2 y$

$m = (ak_1 + k_2)y$

$m = ky$

So, $y|m$, and since $y|n$, we know y is also a common divisor of m and n. So from the definition of greatest common divior, since x = gcd(m, n), we have $y \leq x$.

Because of the previous deduction that $x \leq y$ and $y \leq x$, we know that x = y.

Therefore, $\forall a, m, n \in \mathbb{Z}, x = y$, that is, $\forall a, m, n \in \mathbb{Z}, gcd(m, n) = gcd(m, m - an)$ $\square$

(b)

Proof. We want to disprove the statement.

The statement is: $\forall a, m, n \in \mathbb{Z}, gcd(m, n) = gcd(n, m - an)$ The negation is:$\exists a, m, n \in Z, gcd(n, m) \neq gcd(m, m - an)$. And we want to prove the negation.

Let a = 2, m = 20, n = 5, then m - an =10

Then gcd(m, n) = gcd(20, 5) = 5, gcd(m, m - an) = (20, 10) = 10 by definiton of greatest common advisor.

So, $gcd(m, n) \neq gcd(20, 5)$

So, the negation is True. Hence, the statemnt: $\forall a, m, n \in \mathbb{Z}, gcd(m, n) = gcd(m, m - an)$ is False. $\square$

(c)

Proof. We want to prove: $\forall m, n \in \mathbb{Z}, \exists k \in \mathbb{Z}, m = 2k + 1 \Rightarrow gcd(m, n) = gcd(m, 2n)$.

Let $m, n \in \mathbb{Z}$. Assume $\exists k \in \mathbb{Z}, m = 2k + 1$.

Because $1|m, 1|n, 1|2n$, so m and n at least have a common divisor 1, m and 2n at least have a common divisor 1.

So, assume x = gcd(m, n), y = gcd(m, 2n).

Hence, all we want to show is that x = y, i.e, $x \leq y$ and $y \leq x$.

1. Want to show $x \leq y$:

Because x = gcd(m, n)

Then, $\exists k_1, k_2 \in \mathbb{Z}$, $m = k_1 x$ and $n = k_2 x$.

Let $c = 2k_2$

We have $n = k_2 x$

So, $2n = 2K_2 x$

Therefore, $2n = cx$

So, $x|2n$. And we already know that $x|m$ because x = gcd(m, n). So, x is also a common divisor of m and 2n.

And since y = gcd(m, 2n), by definiton of greatest common divisor, we know that $x \leq y$

2. Want to show $y \leq x$:

The contrapositive of Fact 1 is: $\forall a, b, c \in N, a \nmid c \Rightarrow a \nmid b \vee b \nmid c$.

And let a = 2, b = y, c = m.

Because m is odd, so $2 \nmid m$, and we know that $y|m$, i.e,$\neg(y|m)$, so, $2 \nmid y$. In other words, y is an odd number.

Since y = gcd(m, 2n), $\exists k_1, k_2 \in \mathbb{Z}, m = k_1 y, 2n = k_2 y$.

Because $2n = k_2 y$ is equivalent to $k_2 y = 2 \times n$. And $n \in \mathbb{Z}$. So, $2|k_2 y$.

The contrapositive of Fact 3 is: $\forall a, b, 2|ab \Rightarrow 2|a \vee 2|b$

let a = y, b = k_2.

And because we know y is odd, so $2 \nmid y$, i.e, $\neg(2|y)$ and $2|k_2 y$

So, $2|k_2$, i.e, $\exists k_3 \in \mathbb{Z}, k_2 = 2k_3$.

So, we have $2n = k_2 y = 2k_3 y$.

Then, we get $n = k_3 y$.

Therefore, $y|n$.

And since y is gcd(m, 2n), so $y|m$, so y is also a common divisor of m and n.

And because x = gcd(m, n), from definiton of greatest common divisor, we know that $y \leq x$

Because from the previous deduction that $x \leq y$ and $y \leq x$, we get the conclusion that x = y. That is, gcd(m, n) = gcd(m, 2n).

Then, $\forall m, n \in \mathbb{Z}, \exists k \in \mathbb{Z}, m = 2k + 1 \Rightarrow gcd(m, n) = gcd(m, 2n)$. □

(d)

Proof. $f(n) = n^2 + n + 1$

$f(n + 1) = (n + 1)^2 + (n + 1) + 1 = n^2 + 3n + 3$

So, the statement we want to prove is:$\forall n \in \mathbb{N}, gcd(n^2 + n + 1, n^2 + 3n + 3) = 1$

And from Part(a), we know that $gcd(n^2 + n + 1, n^2 + 3n + 3) = gcd(n^2 + n + 1, 2n + 2)$

Case 1: If n is odd, i.e, $_1 \in \mathbb{N}, n = 2k_1 + 1$

Let $k = 2k_1^2 + 3k_1 + 1$.

Then, we have:

$n^2 + n + 1 = (2k_1 + 1)^2 + (2k_1 + 1) + 1$

$n^2 + n + 1 = 4k_1^2 + 4k_1 + 1 + 2k_1 + 1 + 1$

$n^2 + n + 1 = 4k_1^2 + 6k_1 + 2 + 1$

$n^2 + n + 1 = 2(2k_1^2 + 3k_1 + 1) + 1$

$n^2 + n + 1 = 2k + 1$

So, $n^2 + n + 1 = 2k + 1$ is odd.

Case 2: If n is even, i.e, $_1 \in \mathbb{N}, n = 2k_1$

Let $k = 2k_1^2 + k_1$.

Then, we have:

$n^2 + n + 1 = (2k_1)^2 + 2k_1 + 1$

$n^2 + n + 1 = 4k_1^2 + 2k_1 + 1$

$n^2 + n + 1 = 2(2k_1^2 + k_1) + 1$

So, $n^2 + n + 1 = 2k + 1$ is odd.

Therefore, from previous deduction that whether n is odd or even, $n^2 + n + 1 = 2k + 1$ is odd, so from part(c), we know:

$gcd(n^2 + n + 1, 2n + 2) = gcd(n^2 + n + 1, n + 1)$

And from the conclusion from part a, we know that:$\forall a, m, n \in Z, gcd(m, n) = gcd(n, m - an)$

And we know that since $n \in \mathbb{N}$, so $n^2 + n + 1, n + 1 \in \mathbb{Z}$, so, we have:

$gcd(n^2 + n + 1, n + 1) = gcd(n + 1, n^2 + n + 1 - n \times (n + 1)) = gcd(n + 1, 1) = 1$

Therefore,$gcd(n^2 + n + 1, n + 1) = 1$, and from our previous deduction that $gcd(n^2 + n + 1, n^2 + 3n + 3) = gcd(n^2 + n + 1, n + 1))$, we get $gcd(n^2 + n + 1, n^2 + 3n + 3) = 1$, i.e, gcd(f(n), f(n+1)) = 1.

$\square$

3 Eventually bounded

(a)

Proof. Let $n_0 = 0, y = 1, n \in \mathbb{N}$. And assume $n \geq n_0$.

So, we have:

$$f(n) = \frac{1}{n+1}$$
$$f(n) = \frac{n+1-n}{n+1}$$
$$f(n) = 1 - \frac{n}{n+1}$$

Because $n \in \mathbb{N}$ and $n \geq n_0$ and $n_0 = 0$, we know $\frac{n}{n+1} \geq 0$

So, $f(n) \leq 1$

And $f(n_0) = 1$, so $f(n) \leq f(n_0)$.

Therefore, $f(n) = \frac{1}{n+1}$ is eventually bounded. □

(b)

Proof. Let f be an arbitrary f: N $->$ $\mathbb{R}_{\geq 0}$. Assume f is strictly decreasing, i.e,

$\forall x, y \in N, x < y \Rightarrow f(x) > f(y)$

Want to show that f is eventually bounded, i.e, $\exists n_0 \in \mathbb{N}, \exists y \in \mathbb{R}_{\geq 0}, \forall n \in \mathbb{N}, n \geq 0 \Rightarrow f(n) \leq y$

Let $n_0 = 0$, $y = f(n_0)$. Let $n \in \mathbb{N}$ and assume $n \geq 0$.

Case 1: If n = 0:

Then $n_0 = n = 0$

Then $f(n_0) = f(n)$

So, $f(n) \leq f(n_0)$

So, $f(n) \leq y$

Case 2: If $n > 0$:

From the definition of strictly decreasing, i.e, $\forall x, y \in \mathbb{R}, x < y \Rightarrow f(y) < f(x)$

So, since $n, n_0 \in \mathbb{N}$, we know $n, n_0 \in \mathbb{R}$ because $\mathbb{N} \subset \mathbb{R}$.

And because $n_0 < n$, we know that $f(n) < f(n_0)$.

That is, $f(n) \leq f(n_0) \leftrightarrow f(n) \leq y$.

Hence, $f(n) \leq y$.

So, f is eventually bounded. $\square$

(c)

Proof. Let f_1, f_2 be two arbitrary eventually bounded functions. By the definiton of eventually bounded function, we know that there exists $n_1 \in \mathbb{N}, y_1 \in \mathbb{R}_{\geq 0}$ such that $\forall n \in \mathbb{N}, n \geq n_0 \Rightarrow f_1(n) \leq y_1$ and $n_2 \in \mathbb{N}, y_2 \in \mathbb{R}_{\geq 0}$ such that $\forall n \in \mathbb{N}, n \geq n_2 \Rightarrow f_2(n) \leq y_2$

Let $n_0 = n_1 + n_2$, $y = y_1 \times y_2$.

Let $n \in \mathbb{N}$. Assume that $n \geq n_0$.

Because we know that $n_1, n_2 \in \mathbb{N}$, so $n_0 \geq n_1$ and $n_0 \geq n_2$.

So, since $n \geq n_0$ and f_1, f_2 are two eventually bounded functions, we know that: $f_1(n) \leq f_1(n_0) \leq f_1(n_1)$, $f_2(n) \leq f_2(n_0) \leq f_2(n_2)$.

That is, $f_1(n) \leq y_1$, $f_2(n) \leq y_2$.

So, $f_1(n) \cdot f_2(n) \leq y_1 y_2$

That is, $(f_1 \times f_2)(n) = f_1(n) \cdot f_2(n) \leq y$.

So, $f_1 \times f_2$ is eventually bounded.

Therefore, for every two eventually bounded functions f1, f2: $\mathbb{N} - > \mathbb{R}_{\geq 0}$, the function $f_1 \times f_2$ is also eventually bounded. $\square$