

# CompSci 10M3

## Assignment 4

Q1)

$$45617 = (11^2) \cdot (13) \cdot (29)$$

---

Q2)

$$\gcd(2^{89}, 2^{346})$$

largest divisor of  $2^{89}$  is  $2^{89}$

largest divisor of  $2^{346}$  is  $2^{346}$

because both of them are powers of two

$$\text{then } \gcd(2^{89}, 2^{346}) = 2^{\min(89, 346)}$$

therefore the  $\gcd(2^{89}, 2^{346})$  is  $2^{89}$

---

Q3)

let  $x$  be 33:

$$\text{we have } 33 \equiv 1 \pmod{4}$$

$$33 = 3(11) \rightarrow \text{prime factor of } 33$$

$$\text{and we know that } 11 \equiv 3 \pmod{4}$$

So the claim is **False!**

---

Q4)

$$f(n) = n^2 - n + 17$$

$$\text{if } n = 17 \text{ then } f(n) = (17)^2 - 17 + 17$$

$f(n) = 17 \times 17$  which is divisible  
by ⑪ so it is not a prime  
number  $\longrightarrow$  False

Q5)

$$\text{if } p = 5 \text{ and } q = 11$$

$$\text{then } pq + 1 = (5)(11) + 1 = 56$$

and 56 is divisible by 2, 4, and 13  
so it is not prime  $\longrightarrow$  False

Q6)

$$\gcd(128, 729)$$

$$729 = 5 \cdot 128 + 89$$

$$128 = 1 \cdot 89 + 39$$

$$89 = 2 \cdot 39 + 11$$

$$39 = 3 \cdot 11 + 6$$

$$11 = 1 \cdot 6 + 5$$

$$6 = 1 \cdot 5 + \textcircled{1} \rightarrow \text{last non-zero remainder}$$

$$5 = 5 \cdot 1 + 0$$

So the  $\gcd(128, 729)$  is ⑪

Q7)

$$\gcd(450, 120)$$

$$450 = 3 \cdot 120 + 90$$

$$120 = 1 \cdot 90 + 30 \rightarrow \gcd$$

$$90 = 3 \cdot 30 + 0$$

$$\text{therefore: } 30 = 120 - 1 \cdot 90$$

$$30 = 120 - 1 \cdot (450 - 3 \cdot 120)$$

$$30 = 120 + 3 \cdot 120 - 1 \cdot 450$$

$$30 = 4 \cdot 120 - 1 \cdot 450$$

Q8)

$$\gcd(177, 919)$$

$$919 = 5 \cdot 177 + 34$$

$$177 = 5 \cdot 34 + 7$$

$$34 = 4 \cdot 7 + 6$$

$$7 = 1 \cdot 6 + 1 \rightarrow \gcd$$

$$6 = 6 \cdot 1 + 0$$

therefore:

$$1 = 7 - 1 \cdot 6$$

$$1 = 7 - 1 \cdot (34 - 4 \cdot 7) = 5 \cdot 7 - 1 \cdot 34$$

$$1 = 5 \cdot (177 - 5 \cdot 34) - 1 \cdot 34$$

$$1 = 5 \cdot 177 - 26 \cdot 34$$

$$1 = 5 \cdot 177 - 26 \cdot (919 - 5 \cdot 177)$$

$$1 = 5 \cdot 177 - 26 \cdot 919 + 130 \cdot 177$$

$$1 = 135 \cdot 177 - 26 \cdot 919$$

So the coefficients are 135

and -26, therefore 135

is the inverse of 177 modulo 919.

$$177 \times 135 \equiv 1 \pmod{919}$$

Q9)  $31x \equiv 57 \pmod{61}$

first, we have to find the inverse of 31 modulo 61

we have to find  $\gcd(31, 61)$  first.

$$61 = 1 \cdot 31 + 30$$

therefore:

$$31 = 1 \cdot 30 + 1 \rightarrow \gcd$$

$$1 = 31 - 1 \cdot 30$$

$$30 = 30 \cdot 1 + 0$$

$$1 = 31 - 1 \cdot (61 - 1 \cdot 31)$$

$$1 = 2 \cdot 31 - 61$$

So the coefficients are 2 and -1

and the inverse of 31 modulo 61 is 2

if we multiply both sides of the congruence by the inverse we get:

$$2 \times 31x \equiv 2 \times 57 \pmod{61}$$

as we know  $2 \times 31 \equiv 1 \pmod{61}$  so therefore

$$x \equiv 2 \times 57 \pmod{61}$$

$$x \equiv 114 \pmod{61}$$

$$x \equiv 53 \pmod{61}$$

---

Q10) imagine we have a three digit number

$$abc \xrightarrow{s} abc = (a \times 100) + (b \times 10) + c$$
$$abc = 100a + 10b + c$$

and the number cba is going to be:

$$cba = 100c + 10b + a$$

$$\text{therefore } abc - cba = (100a + 10b + c) - (100c + 10b + a)$$

$$abc - cba = 99a - 99c$$

$$abc - cba = 99(a - c)$$

$$abc - cba = 9 \times 11 \times (a - c)$$

So it's always divisible by 9

Q11) prove  $\sum_{j=n}^{2n-1} (2j+1) = 3n^2$  for all positive integers.

base case: for  $n=1$ , the sum has only one term:

$$\sum_{j=1}^1 (2j+1) = 2(1)+1 = 3 \quad \text{and the right hand side}$$

$$\text{of the equation is } 3(1)^2 = 3$$

therefore it's true for the base case

inductive hypothesis: we assume the statement is true for some positive integer  $n=k$

$$\sum_{j=k}^{2k-1} (2j+1) = 3k^2$$

inductive step:

prove the statement holds for  $n = K+1$ , meaning:

$$\sum_{j=K+1}^{2(K+1)-1} (2j+1) = 3(K+1)^2$$

we expand the left side:

$$\sum_{j=K+1}^{2(K+1)-1} (2j+1) = \sum_{j=K}^{2K-1} (2j+1) + \sum_{j=2K}^{2K+1} (2j+1)$$

from the inductive hypothesis:

$$\sum_{j=K+1}^{2(K+1)-1} (2j+1) = 3K^2$$

therefore we would have:

$$\begin{aligned} \sum_{j=K+1}^{2(K+1)-1} (2j+1) &= 3K^2 + (2(2K)+1) + (2(2K+1)+1) \\ &\quad - (2K+1) = 3K^2 + 6K + 3 \\ &= 3(K+1)^2 \therefore \text{proven!} \end{aligned}$$

Q12)  $a_1=2$ ,  $a_2=9$ , and  $a_n=2a_{n-1}+3a_{n-2}$   $n \geq 3$

prove  $a_n \leq 3^n$  for all positive integers  $n$

base case  $n=1$ :

$$a_1=2, 2 \leq 3^1 \checkmark$$

$$a_2=9, 9 \leq 3^2 \checkmark$$

$\therefore$  the base case is true

induction hypothesis:

we assume

$$a_n \leq 3^n$$

inductive step: we have to prove that

$$a_{n+1} \leq 3^{n+1}$$

$$a_{n+1} = 2a_n + 3a_{n-1}$$

$$a_{n+1} \leq 2(3^n) + 3(3^{n-1})$$

$$a_{n+1} \leq 2(3^n) + 3(3^n)$$

$$a_{n+1} \leq 2(3^n) + 3^n$$

$$a_{n+1} \leq (2+1)3^n$$

$$a_{n+1} \leq 3(3^n)$$

$$a_{n+1} \leq 3^{n+1}$$

Q13) prove  $4 \mid (9^n - 5^n)$  for all  $n \geq 0$

base case:  $n=0$

$$4 \mid (9^0 - 5^0)$$

$$4 \mid 0 \text{ true } \checkmark$$

induction step:

now we have to prove its true for  $n+1$  (next page!)

induction hypothesis:

we assume the statement is true for  $n$

$$4 \mid (9^n - 5^n) \text{ so } 9^n - 5^n = 4m$$

$$4 \mid (9^{n+1} - 5^{n+1})$$

$$\equiv 4 \mid (9 \cdot 9^n - 5 \cdot 5^n)$$

$$9^{n+1} - 5^{n+1} = (9 \cdot 9^n - 9 \cdot 5^n) + (9 \cdot 5^n - 5 \cdot 5^n)$$

$$9^{n+1} - 5^{n+1} = 9(9^n - 5^n) + 5^n(9 - 5)$$

$$9^{n+1} - 5^{n+1} = 9 \underbrace{(9^n - 5^n)}_{4m} + 4 \cdot 5^n$$

$$9^{n+1} - 5^{n+1} = 9(4m) + 4 \cdot 5^n$$

$$9^{n+1} - 5^{n+1} = 4(9m) + 4 \cdot 5^n$$

$$9^{n+1} - 5^{n+1} = 4(9m + 5^n)$$

divisible by 4

So we conclude that  $4 \mid 9^{n+1} - 5^{n+1}$  therefore

The statement  $4 \mid 9^n - 5^n$  for  $n \geq 0$  is proven to be true.