MTH3121 Problem Sheet 7 : Saral 30 618 428

Question 2

a) So we are told that :
$333\,x \equiv 6 \bmod 3003$ (Modulo 2.0)

To solve this we can firstly divide both sides by gcd $(333, 3003) = 3$, to get :

$111\,x \equiv 2 \bmod 1001$ (Modulo 2.1)

Now multiply both sides by $111^{-1} = 496$:

$x \equiv 992 \bmod 1001$ (Modulo 2.2)

Thus $x = 992, 1993, 2994$

b) So we are told that :

$2121\,x \equiv 2021 \bmod 1001$ (Modulo 2.3)

This congruence has no solutions since gcd $(2121, 1001) = 7$, does not divide 2021.

Question 4

If we add $(3121^{2021} - 3)$ and $(3121^{2021} + 3)$ together then we get :

$(3121^{2021} - 3) + (3121^{2021} + 3) = 2\,(3121^{2021})$ (Equation 4.0)

Now according to theorem 6 the lecture slides :

' Fix integers a, b, c. There exists x,
$y \in \mathbb{Z}$ such that $c = ax + by$ if and only if gcd $(a, b) \mid c$ ' (Theorem 6)

This means Equation 4.0 is only possible if gcd $(3121^{2021} - 3, 3121^{2021} + 3)$ divides $2\,(3121^{2021})$.

Now how can this be possible ?

Possibility 1 : gcd $(3121^{2021} - 3, 3121^{2021} + 3)$ is 3121^{z}, where $z \geq 0$.

Now this is not possible since the difference between $3121^{2021} - 3$ and $3121^{2021} + 3$ is 6. If the difference between them is 6, then 3121 cannot divide both of them.

So the only possible answer in this case is that gcd $(3121^{2021} - 3, 3121^{2021} + 3) = 1$

Possibility 2 : gcd $(3121^{2021} - 3, 3121^{2021} + 3)$ is a divisor of 2.

Let ' s first establish some basic rules with numbers :

odd x odd = odd (Equation 4.1)

odd $\pm$ odd = even (Equation 4.2)

This means that :

$3121^{2021} - 3$ = odd − odd = even (Equation 4.3)

$3121^{2021} + 3$ = odd + odd = even (Equation 4.4)

Since $3121^{2021} - 3$ and $3121^{2021} + 3$ are both even we know that 2 divides both of them.

So we have that 2 divides both $3121^{2021} - 3$ and $3121^{2021} + 3$ and that $\gcd\left(3121^{2021} - 3,\ 3121^{2021} + 3\right)$ is a divisor of 2.

Therefore :

$\gcd\left(3121^{2021} - 3,\ 3121^{2021} + 3\right) = 2$

Quesiton 6

Let ' s first go through what we know.

$S = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : ax + by = c\}$

We are told to consider two solutions (x_0, y_o) and (x_1, y_1) that are in S and that :

$x_1 = x_0 + u$ (Equation 6.0)

$y_1 = y_0 - v$ (Equation 6.1)

So we can rewrite (x_1, y_1) as :

$(x_0 + u, y_0 - v)$ (Pair 6.2)

For (x_0, y_0) and $(x_0 + u, y_0 - v)$ to be in S :

$ax_0 + by_0 = c$ (Equation 6.3)

$a(x_0 + u) + b(y_0 - v) = c$ (Equation 6.4)

Expanding the brackets in Equation 6.4, we find that :

$ax_0 + by_0 + au - bv = c$ (Equation 6.5)

Substituting Equation 6.3 into Equation 6.5, gives the result :

$c + au - bv = c$ (substituting Equation 6.3)

$au - bv = 0$ (subtracting c from both sides)

$au = bv$ (adding bv to both sides) (Equation 6.6)

Making u the subject of Equation 6.6 :

$u = \frac{bv}{a}$ (Equation 6.7)

Making v the subject of Equation 6.6 :

$v = \frac{au}{n}$ (Equation 6.8)

Thus (x_1, y_1) can again be written as :

$\left(x_0 + \frac{bv}{a},\ y_0 - \frac{au}{n}\right)$ (Pair 6.9)

So what we just found was that any solution in S can be written as :

$$\left(x_0 + \frac{bv}{a},\ y_0 - \frac{au}{n}\right)$$

Therfore we can rewrite the set S as :

$$S = \left\{\left(x_0 + \frac{bv}{a},\ y_0 - \frac{au}{n}\right) \text{ where } x_0,\ y_0,\ b,\ v,\ a,\ u \text{ are all integers}\right\}$$

If we set $\frac{bv}{a} = te$ and $\frac{au}{n} = tf$, then :

$$\frac{bv}{ae} = \frac{au}{bf} \quad \text{(Equation 6.10)}$$

Putting e/f on one side of Equation 6.10 :

$$\frac{b^2 v}{a^2 u} = \frac{e}{f} \quad \text{(Equation 6.11)}$$

So we have shown that e and f both depend on the values of
a and b and using the value of t we set before we can rewrite S as :

$$S = \left\{\left(x_0 + te,\ y_0 - tf\right) \text{ where t is an integer}\right\}$$

Question 8

Again using theorem 6 from the lecture slides :

' Fix integers a, b, c. There exists x,
$y \in Z$ such that $c = ax + by$ if and only if $\gcd(a, b) \mid c$ ' (Theorem 6)

So for the equations :

$$94x + 235y = n \quad \text{(Equation 8.0)}$$

$$344u + 129v = n \quad \text{(Equation 8.1)}$$

Theorem 6 would mean that :

$$\gcd(94,\ 235) \mid n \text{ and } \gcd(344,\ 129) \mid n \quad \text{(Statement 8.2)}$$

$$\gcd(94,\ 235) = 47 \text{ and } \gcd(344,\ 129) = 43$$

So this means that n is divisible by both 43 and 47.

Since 43 and 47 are prime, the smallest positive integer that is divisible by both 43 and 47 is :

$$43 \times 47 = 2021$$

The values hat give 2021 as n in Equation 8.0 and Equation 8.1 are :

$$x = 9,\ y = 5,\ u = 1,\ v = 13$$

Question 10

So we have to find for which pairs of positive integers (a, b) the statement :

$\gcd(c, ab) = \gcd(c, a)\gcd(c, b)$ for all $c \in \mathbb{N}$ (Statement 10.0)

would be true.

From Statement 10.0 we know that $\gcd(c, a)$ and $\gcd(c, b)$ are divisors of $\gcd(c, ab)$.

Now according to Theorem 6 :

' Fix integers a, b, c. There exists x,
$y \in Z$ such that $c = ax + by$ if and only if $\gcd(a, b) \mid c$ ' (Theorem 6)

Therefore :

$\gcd(c, ab) = ce + af$, where e and a are integers (Equation 10.1)

$\gcd(c, ab) = cg + bh$, where g and h are integers (Equation 10.2)

We also know from Statement 10.0 that gcd
(c, ab) is a divisor of $\gcd(c, a)\gcd(c, b)$, therefore :

$\gcd(c, a)\gcd(c, b) = ci + abj = \gcd(c, ab)$, where i and j are integers (Equation 10.3)

By equating Equation 10.1, 10.2 and 10.3 we have the result that :

$ce + af = cg + bh = ci + abj$ (Equation 10.4)

Now how is Equation 10.4 possible ?

By equating coefficients for c we know that :

$e = g = i$ (Equation 10.5)

And by equating coefficients for a and b :

$f = bj$ (Equation 10.6)

$h = aj$ (Equation 10.7)

Dividing Equation 10.6 by Equation 10.7, gives the result :

$\frac{f}{h} = \frac{b}{a}$ (Equation 10.8)

And multiplying both sides by ' a ' in Equation 10.8 :

$b = \frac{f}{h} a$ (Equation 10.9)

Thus if $(a, b) = \left(a, \frac{f}{h} a\right)$, then for all $c \in \mathbb{N}$:

$\gcd(c, ab) = \gcd(c, a)\gcd(c, b)$

where f and h are integer solutions to :

$af = bh$.