[4] **0. Definitions**

(a) Define what it means for an integer a to divide an integer b.

We say that a divides b (written $a|b$) if there is an integer k s.t.

$$b = ak.$$

(b) What does it mean for two integers to be relatively prime? Provide an example.

Two integers a, b are relatively prime if $\gcd(a,b) = 1$.

Example: 2, 3.

[5] 1. Show that if $[x]_b = [y]_b$ for an integer $b \neq 0$, and integers x, y, then we have that

b divides $(x - y)$.

Proof 1: We write $x = q_1 b + r_1$, $y = q_2 b + r_2$.

Then $[x]_b = [y]_b$ implies that $r_1 = r_2$.

Thus: $x - y = (q_1 b + r_1) - (q_2 b + r_2)$

$$= (q_1 - q_2) b + \underbrace{(r_1 - r_2)}_{=0}$$

$$= (q_1 - q_2) b$$

And since $q_1 - q_2$ is an integer, we see that $b \mid (x - y)$.

Proof 2: Since $[x]_b = [y]_b$, we have that

$[x - y]_b = [x]_b - [y]_b = [0]_b$

But this is equivalent to the remainder being 0 i.e. $(x - y) = kb$

or: b divides $x - y$. $\square$

[5] **2**. Prove or disprove that for every integer n, the integers $2n+1$ and $3n+1$ are relatively prime.

This is true. ~~We~~

Proof 1: If $d \mid 2n+1$ and $d \mid 3n+1$

then $d \mid (3n+1)-(2n+1) = n$

Similarly, $d \mid \underbrace{2\cdot(2n+1) - (3n+1)}_{n+1}$

and so $d \mid n$ and $d \mid n+1$. But this is true iff $d = 1$.

Thus the greatest common divisor is 1.

Proof 2: We note that

$$3(2n+1) + (-2)(3n+1) = 1.$$

Since 1 is a linear combination of $2n+1$ and $3n+1$, it follows that the gcd is also 1.

$\square$

[6] **3.**

(a) Prove that every two consecutive integers of the form $4k+1$ are relatively prime (for example: 5, 9 are consecutive of this form).

let $d = \gcd(4k+1, 4k+5)$.

Then $d \mid \underbrace{(4k+5)-(4k+1)}_{=4}$

i.e. d is 1, 2, or 4.

However, $4k+1$ is odd, so neither 2 nor 4 divide it. Thus $d=1$ as claimed.

(b) Is the same true of those of the form $4k+2$?

No. $4k+2$ and $4k+6$ are both divisible by 2.

[5] **4**. Find all strictly positive integer solutions to the equation

$$x^2 - y^2 = 9.$$

(Hint: Consider factoring the left-hand side.)

We factor the LHS: $(x+y)(x-y) = 9$

As $x+y$, $x-y$ are both integers,

we need one of 3 possibilities:

1) $x+y = 1$, $x-y = 9$

subtract ~~Adding~~ these gives $2y = -8$

$\Rightarrow y < 0$ ↯

2) $x+y = 3$, $x-y = 3$

Subtracting these yields $2y = 0$ ↯

3) $x+y = 9$, $x-y = 1$

Adding these gives $2x = 10 \Rightarrow x = 5$

$\Rightarrow y = 4$

So the only such solution is

$x = 5$ and $y = 4$.

[6] **5.** Consider the following theorem.
Theorem If a and b are relatively prime, and if $a \mid c$, and $b \mid c$, then we have that $ab \mid c$.

(a) Show with an example that if a and b are *not* relatively prime, then there is a c with $a \mid c$ and $b \mid c$ such that $ab \nmid c$.

If we choose $a = b = c = 2$,
then $a|c$, $b|c$, but $ab = 4$
does <u>not</u> divide c.

(b) Prove the given theorem.

If a, b are relatively prime then there are integers s, t such that $as + tb = 1$. ①
Moreover, as $a|c$ and $b|c$ there are integers m, n such that $c = ma$ and $c = nb$.
Then multiplying ① by c we find

$$c = asc + tbc = as(nb) + tb(ma)$$
$$= asnb + tbma = ab(sn + tb)$$

Thus $ab|c$ as claimed. $\square$