(1) (Niven 5.3.3) Find all PT's whose terms form an

(a) Arithmetic progression
Such a triple would be of the form $(b-d, b, b+d)$ for $b, d \in \mathbb{Z}^+$. To be Pythagorean triples, we require

$$\begin{aligned}(b-d)^2 + b^2 &= (b+d)^2\\ 2b^2 - 2bd + d^2 &= b^2 + 2bd + d^2\\ b^2 &= 4bd\\ b &= 4d.\end{aligned}$$

Thus the PT's that are arithmetic progressions are exactly those of the form $(3d, 4d, 5d)$ for $d \in \mathbb{Z}^+$.

(b) Geometric progression
Such a triple would be of the form (a, ar, ar^2) for $a \in \mathbb{Z}^+$ and $r \in \mathbb{Q}$. So we would have

$$\begin{aligned}a^2 + a^2r^2 &= a^2r^4\\ a^2(1+r^2) &= a^2r^4\\ r^4 - r^2 - 1 &= 0.\end{aligned}$$

So the quadratic formula gives that $r^2 = \dfrac{1+\sqrt{5}}{2}$, but this gives $r \notin \mathbb{Q}$, so there are no PT's in a geometric progression.

(2) (Niven 5.3.7) For which n are there solutions to $n = x^2 - y^2$?

First, for n odd, we can write $n = 2k+1$ for $k \in \mathbb{Z}$. Then let $x = k+1$ and $y = k$. Then we get

$$x^2 - y^2 = (k+1)^2 - (k)^2 = k^2 + 2k + 1 - k^2 = 2k + 1 = n.$$

Next, for n even, we split it into two subcases. First suppose 4 divides n, so $n = 4k$. If we let $x = k+1$ and $y = k-1$,

$$x^2 - y^2 = (k+1)^2 - (k-1)^2 = k^2 + 2k + 1 - (k^2 - 2k + 1) = 4k = n.$$

If instead n is even but not divisible by 4, there is a simple proof that n cannot be written as a difference of squares looking at the number mod 4. The set of squares mod 4 are $\{0, 1\}$, and a difference of two elements of that set can only give 0 or ± 1.

Thus those n that can be written as a difference of squares are exactly the n not congruent to 2 mod 4.

(3) (Niven 5.3.9) Prove that any integer n can be expressed in the form

$$n = x^2 + y^2 - z^2.$$

This is easily proved from the previous problem. If we let $x = 0$, we have shown that there are integers y and z satisfying the equation for all n not congruent to 2 mod 4. In this last case, instead let $x = 1$. Then $n - 1$ is congruent to 1 mod 4, so there are y and z with

$$y^2 - z^2 = n - 1,$$

from the last problem. This gives the solution, so we are done.

(4) Find [sic] all PPT's with $c = a + 2$.

We want to find integers a and b such that

$$a^2 + b^2 = (a + 2)^2.$$

Expanding the right side and canceling gives

$$b^2 = 4a + 4.$$

So b must be even. Say $b = 2k$. Then the triple that can be formed is

$$(a, b, c) = (k^2 - 1, 2k, k^2 + 1).$$

These are the only such triples, and they give triples for all $k > 1$.

(5) The n-th *triangular number* is given by $T_n := 1 + 2 + \cdots + n$.

(a) Prove using induction that $T_n = \dfrac{n(n+1)}{2}$.

The base case is easy: $T_1 = 1 = \dfrac{1(2)}{2}$. Now for the inductive step.

Assume $T_n = \dfrac{n(n+1)}{2}$. Then we have the following series of equalities:

$$T_{n+1} = 1 + 2 + \cdots + n + (n + 1) = T_n + (n + 1) =$$
$$= \frac{n(n+1)}{2} + (n + 1) = \frac{n(n+1) + 2n + 2}{2} = \frac{(n+1)(n+2)}{2}.$$

This completes the inductive step, so by induction, the formula holds for all positive integers n.

(b) Prove that for any n there is a PPT containing $4T_n$.

It is easy to see that $(2n + 1, 2n(n + 1), 2n(n + 1) + 1)$ is a PPT. It is primitive because the last two entries differ by 1. Finally, by the previous part, the middle term is exactly the formula for $4T_n$.

(6) Prove that

$$\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}.$$

This is also done using induction. The base case can be cleverly chosen to be $n = 0$, this corresponds to an empty sum on the left (zero) and $\frac{0}{1}$ on the right. Using the base case $n = 1$ also works just fine.

The inductive step starts by assuming the equation for n. Now adding the next term to both sides, we have

$$\sum_{i=1}^{n} \frac{1}{i(i+1)} + \frac{1}{(n+1)((n+1)+1)} = \frac{n}{n+1} + \frac{1}{(n+1)((n+1)+1)} = \frac{n(n+2)+1}{(n+1)(n+2)} =$$
$$= \frac{n^2+2n+1}{(n+1)(n+2)} = \frac{(n+1)^2}{(n+1)(n+2)} = \frac{n+1}{n+2}.$$

This proves the inductive step, so by induction the formula holds for all $n \in \mathbb{Z}^+$.

(7) (a) Find all rational points on the circle $x^2 + y^2 = 2$, using $(1, 1)$ as the starting point.
This is done by fixing a line with rational slope a through $(1, 1)$ and finding the second point of intersection (x, y) of the line with the circle. This involves some simple algebra, the simultaneous solution of the two equations

$$\frac{y-1}{x-1} = a$$
$$x^2 + y^2 = 2.$$

This solves to give you the trivial solution $x = y = 1$ and the point sought after:

$$(x, y) = \left(1 - \frac{2(a+1)}{a^2+1}, 1 - \frac{2a(a+1)}{a^2+1}\right).$$

(b) Try to use the same method to find all rational points on $x^2+y^2 = 3$. What goes wrong?
The problem here is that there is no point to start with. As such, any line with rational slope can simply intersect the circle at two points that each have irrational coordinate(s). Without the basepoint, we don't know that the other point will give us a point with two rational coordinates. As the (Bonus) suggests, it turns out there is no rational point on this circle!
The argument to use here is to show that a solution in rationals would give an integer solution to $x^2 + y^2 = 3z^2$, and this can be chosen with the x, y, and z not all sharing a common factor. Now look at this equation mod 4.

(8) (Niven 1.2.2) Find the greatest common divisor $g = (1819, 3587)$, and find x, y such that

$$1819x + 3587y = g.$$

The Euclidean algorithm gives the following:

$$\begin{aligned} 587 &= 1819 \cdot 1 + 1768 \\ 1819 &= 1768 \cdot 1 + 51 \\ 1768 &= 51 \cdot 34 + 34 \\ 51 &= 34 \cdot 1 + 17 \\ 34 &= 17 \cdot 2. \end{aligned}$$

So $g = 17$. Working backwards through the algorithm, we get

$$1819 \cdot (71) + 3587 \cdot (-36) = 17.$$

(9) (Niven 1.2.9) Show that if $ac|bc$, then $a|b$.

$ac|bc$ means $\exists x \in \mathbb{Z}$ such that $(ac)x = (bc)$. Then $(ax)c = bc$ which implies $ax = b$, or $a|b$.

(10) (Niven 1.2.10) Show that if $a|b$ and $c|d$, then $ac|bd$.

$a|b$ and $c|d$, so $\exists x, y \in \mathbb{Z}$ with $ax = b$ and $cy = d$. Multiplying these two equations gives

$$bd = (ax)(cy) = (ac)(xy).$$

Thus, $ac|bd$.

(11) (Niven 1.2.11) Prove that $4 \not| (n^2+2)$ for any n. Suppose first that n is odd. Then $n = 2k+1$ for some $k \in \mathbb{Z}$. This gives

$$(n^2 + 2) = (2k+1)^2 + 2 = 4k^2 + 4k + 1 + 2 = 4(k^2 + k) + 3.$$

Thus if $4|(n^2 + 2)$, then $4|3$, which is clearly false. So this case is finished.

If instead n is even, $n = 2k$. So

$$(n^2 + 2) = (2k)^2 + 2 = 4k^2 + 2.$$

So here, if $4|(n^2 + 2)$, then $4|2$, again a contradiction. Therefore for any n, $4 \not| (n^2 + 2)$.

(12) (Niven 1.2.12) Given that $(a, 4) = (b, 4) = 2$, prove that $(a + b, 4) = 4$.

Since $(a, 4) = 2$, $2|a$, so $a = 2m$ for $m \in \mathbb{Z}$. But we also know $4 \not| a$, so $2 \not| m$, and so $m = 2n + 1$ for $n \in \mathbb{Z}$. This gives $a = 4n + 2$, and similarly $b = 4k + 2$ for some $k \in \mathbb{Z}$. So we now have that

$$a + b = (4n + 2) + (4k + 2) = 4n + 4k + 4 = 4(n + k + 1)$$

So $4|(a + b)$, which shows that $(a + b, 4) = 4$.

(13) (Niven 1.2.17) Evaluate $(n, n + 1)$ and $[n, n + 1]$.

Any common divisor of n and $n + 1$ would have to divide their difference, which is 1. Therefore $(n, n + 1) = 1$.

Suppose $[n, n + 1] = an = b(n + 1)$. Then

$$b = an - bn = (a - b)n.$$

This shows $n|b$, so the least common multiple is at least $n(n + 1)$. But this is obviously a common multiple, so $[n, n + 1] = n(n + 1)$.

(14) (Niven 1.2.36) Prove that $(a, b, c) = ((a, b), c)$.

The left side is the greatest positive integer that divides a, b, and c. Thus it divides (a, b), by Theorem 1.4, so is no more than the right side. But the right side clearly divides (a, b), so it divides a and b, by transitivity, as well as c, so is less than or equal to the left side. Therefore the two sides are equal.

(15) (Niven 1.2.43) Prove that $a|bc$ if and only if $\frac{a}{(a,b)}|c$.

($\Rightarrow$) We have $a|bc$, so $ax = bc$ for some $x \in \mathbb{Z}$. Letting $g = (a, b)$, we know g divides a and b, so we can write $mgx = ngc$ for integers m, n. So $mx = nc$ (or $m|nc$) and $(m, n) = 1$, since otherwise g was not the greatest common divisor of a and b. So Theorem 1.10 gives that $m|c$. But by construction, $m = \dfrac{a}{(a, b)}$, so we are done.

($\Leftarrow$) If $\frac{a}{(a,b)}|c$, then multpilying both by (a, b) gives that $a|(a, b)c$. Now, by transitivity, since $(a, b)|b$, $a|bc$.

(16) Prove that in the Euclidean algorithm, $r_{i+2} < \frac{1}{2}r_i$.

We can break this into cases: first assume that $r_{i+1} \leq \frac{1}{2}r_i$. Then since the remainders strictly decrease, we have $r_{i+2} < r_{i+1} \leq \frac{1}{2}r_i$, so we are done.

Now, if instead $r_{i+1} > \frac{1}{2}r_i$, let's carry out the divsion of r_i by r_{i+1}.

$$r_i = r_{i+1} \cdot 1 + (r_i - r_{i+1})$$

This is the division because we know $2r_{i+1} > r_i$. So

$$r_{i+2} = r_i - r_{i+1} < r_i - \frac{1}{2}r_i = \frac{1}{2}r_i.$$

So we have proven it for each case.

This gives the bound on the total number of steps equal to $2\lceil \log_2(n) \rceil$, for n the first dividend, since we know every two steps the remainders are at most half of what they were.

(17) (Niven 1.2.45) Prove that any positive integer a can be uniquely expressed as

$$a = 3^m + b_{m-1}3^{m-1} + \cdots + b_1 3 + b_0,$$

where $b_i = 0, 1$ or -1.

One way to show this is by induction on m. What is tricky here is to be sure to formulate your inductive hypothesis correctly. What I want to show is true is that given any n a nonnegative integer, all positive integers less than $\frac{1}{2}3^n$ can be written in the above form, with $m < n$. The base case is easy: we need to show it for integers less than $\frac{1}{2}3^1 = 1.5$, so it is just for $1 = 3^0$.

Now for the inductive step. Assume for that all integers from 1 to $\frac{1}{2}3^n$ can be expressed in the given form. Now we want to show that for any integer M from the range $(\frac{1}{2}3^n, \frac{1}{2}3^n)$, we can write it in that form.

So we have $\frac{1}{2}3^n < M < \frac{1}{2}3^{n+1}$. The inequalities are strict because the fractions will never be integers. Now consider $M - 3^n = M'$. From simple arithmetic, we have

$$-\frac{1}{2}3^n \leq M' < \frac{1}{2}3^n.$$

Therefore, by the inductive step, we have that $|M'| = 3^r + b_{r-1}3^{r-1} + \cdots + b_0$ for $r < n$. This gives that

$$M = 3^n + M' = 3^n \pm |M'| = 3^n \pm 3^r \pm b_{r-1}3^{r-1} \pm \cdots \pm b_0.$$

This shows that M can be written in the necessary form.

To show this form is unique, assume we had

$$3^m + a_{m-1}3^{m-1} + \cdots + a_0 = 3^n + b_{n-1}3^{n-1} + \cdots + b_0,$$

two different representations of the same number, and have it be the example that has the smallest maximal power of 3, say m. Looking at each side, all summands are divisible by 3 except for a_0 and b_0. Therefore $3|(b_0 - a_0)$. But since these two numbers are each $0, 1$ or -1, that shows that in fact $a_0 = b_0$. Subtracting them from each side and dividing by 3 gives

$$3^{m-1} + a_{m-1}3^{m-2} + \cdots + a_2 3 + a_1 = 3^{n-1} + b_{n-1}3^{n-2} + \cdots + b_2 3 + b_1,$$

and this example has a smaller maximal power of 3, namely $m - 1$. This is a contradiction, so there cannot be two different representations of the same number.