Lesson 4: Algebra and remainders.

Konstantin Miagkov

May 4, 2019

Problem 1.
a) The straight line $y = 7x/15 + 1/3$ passes through two intergal points: $(10, 5)$ and $(-20, -9)$. Does it pass through any other integral points?

Proof. Suppose (x_0, y_0) is an integer point, then

$$7 \cdot \frac{x_0 + 15}{15} + \frac{1}{3} = 7 \cdot x_0 + \frac{1}{3} + 7 \cdot \frac{15}{15} = y_0 + 7$$

is also an integer and thus $(x_0 + 15, y_0 + 7)$ is an integer point as well. Therefore another integer point of the graph is $(25, 12)$. □

b) The graph of a function $y = kx + b$ passes through two distinct integral points. Are there any other integral points on this graph?

Proof. First of all, we can ensure that the slope is a rational number since if a line passes through two different integral points (x_0, y_0) and (x_1, y_1) then we can calculate the slope to be

$$k = \frac{y_1 - y_0}{x_1 - x_0}$$

Using the same idea as in part a), we add the denominator of the slope to x to get another integral point. So if we plug in $x_1 + x_1 - x_0$ for x in

$$y = \frac{y_1 - y_0}{x_1 - x_0} \cdot x + b$$

we get

$$\frac{y_1 - y_0}{x_1 - x_0} \cdot (x_1 + x_1 - x_0) + b = \frac{y_1 - y_0}{x_1 - x_0} \cdot x_1 + b + y_1 - y_0 = y_1 + y_1 - y_0$$

which is certainly an integer. Thus, $(2x_1 - x_0, 2y_1 - y_0)$ is another integer point. □

c) Does there exist a linear function $y = kx + b$ such that its graph passes through exactly one integral point?

Proof. Yes. To achieve this, we need to pick a line with an irrational slope. $y = \sqrt{2}x$ works – then if x is a nonzero integer y cannot be an integer since $\sqrt{2} = y/x$ would be rational. Then the only integral point on this line is $(0, 0)$. □

Problem 2.
Solve the equation:

$$\begin{cases} \frac{x}{x+1} + y^2 = 4 \\ y^2 - \frac{5x}{x+1} = -14 \end{cases}$$

Hint: Subtracting the lines and cancelling out y^2 yields a linear equation in x. Once x is known, y is easily recovered. The solutions are $(-3/2, \pm 1)$.

Problem 3.
a) Let a, b be positive integers. Show that their exist unique nonnegative integers q, r such that $a = bq + r$ and $r < b$.

b) Let a, b be integers. Show that there exist unique integers q, r such that $a = bq + r$ and $0 \leq r < |b|$.

First proof. (Existence)
Solution 1: Consider the numbers: 0, b, $2b$, $3b$... After some point, all numbers on the list will be greater than a. For example, ab will be greater than a, and so will all the numbers that follow ab. Let q be the smallest number such that $qb \leq a$. Now we only have to show $a - qb < b$. Suppose that is not true, $a - qb \geq b$. Then $a \geq qb + b = (q+1)b$. This is a contradiction to q being the biggest number such that $qb \leq a$. We can conclude that there exists q and $r = a - qb$ such that $a = qb + r$ with $r < b$.

Solution 2: Let q be the integer part of a/b in decimal. For example if $a/b = 7.6666...$, then $q = 7$. (This can be denoted as $q = \lfloor a/b \rfloor$). Then

$$\frac{a}{b} - q < 1$$

multiplying by $b > 0$ on both sides we get $a - qb < b$, which lets us set $r = a - qb$ and be done.

(Uniqueness) Suppose there is another pair q', r' satisfying the condition. So $a = qb + r$ and $a = q'b + r'$. Subtract one from the other, and we get

$$0 = b(q - q') + r - r' \tag{1}$$

$$b(q - q') = r' - r \tag{2}$$

If $q = q'$ we must also have $r = r'$ by equation (1), which means the pairs wee actually the same. If q and q' are distinct integers, $|b(q - q')| \geq b$. But since $0 \leq r < b$ and $0 \leq r' < b$ we have $|r - r'| \leq b - 1$. Therefore equation (2) cannot hold. Contradiction, so q and r must be unique.

b) To deal with the situation when a and b could be negative, we consider three separate cases:

1) Both a and b are negative. Then we can apply part a) to get

$$(-a) = (-b)q + r$$

for some $0 \leq r < |b|$. Multiplying both sides by -1 we get

$$a = bq - r$$

If $r = 0$, then this is already in the required form. Otherwise, we can also write

$$a = b(q-1) - r - b = b(q-1) + (-b - r)$$

Since b is negative and $1 \leq r < |b|$ we have $0 < -b - r < |b|$ and so

$$a = b(q-1) + (-b - r)$$

is the required form.

2) $a > 0$ and $b < 0$. Then we can apply part a) to get

$$a = (-b)q + r$$

for some $0 \leq r < |b|$. This can be rewritten as

$$a = b(-q) + r$$

which concludes this case.

3) $a < 0$ and $b > 0$. Then we can apply part a) to get

$$-a = bq + r$$

for some $0 \leq r < |b|$. This can be rewritten as

$$a = b(-q) - r$$

If $r = 0$, then this is already in the required form. Otherwise, we can also write

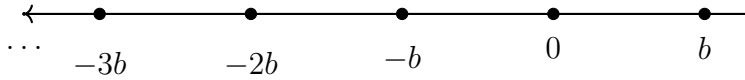
$$a = b(-q-1) - r + b = b(-q-1) + (b - r)$$

Since b is positive and $1 \leq r < |b|$ we have $0 < b - r < |b|$ and so

$$a = b(-q-1) + (b - r)$$

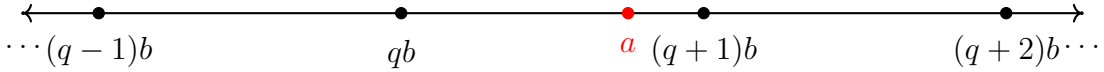
is the required form. □

Second proof. We will give the solution straight for part b) of the problem. First suppose $b > 0$. Then let us mark the points $0, b, 2b, 3b, \ldots$ on the coordinate line. And the same for



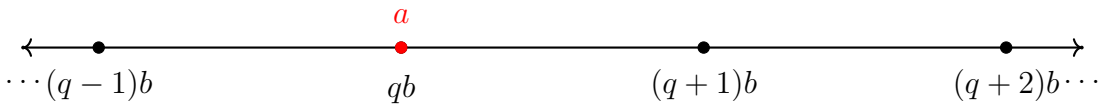
negative multiples of b: $-b, -2b, -3b$ and so on.

If we now represent a as a point on the coordinate line, it will fall between some pair of marked points, lets call them qb and $(q+1)b$.



If a falls

directly on a marked point, we will call that point qb:



Now let us set $r = a - qb$. Since a is between qb and $qb+b$ we know that $r = a-qb < qb+b-qb = b$, so $r < b$ and clearly $r \geq 0$. Thus these r and q work, which concludes the case $b > 0$.

If $b < 0$, we can use the previous case: if we find q and $0 \leq r < |b|$ such that $a = q(-b)+r$, then it also holds that $a = (-q)b + r$ which is the desired formula.

The argument we presented proves that q, b exist. As far as the uniqueness goes, one can either follow the argument in part a) of the original algebraic solution, or consider the following geometric viewpoint: if one chooses $q'b$ to be any point with $q' > q$ where q is the one we chose, then $q'b$ will be to the right of a and $r' = a - q'b$ will have to be negative. If we choose $q' < q$, then the point $q'b$ will be at least length b far from a to the left, and so $r' = a - q'b > b$ which is also prohibited. So the choices of q and r we made were in fact forced, and thus unique. As for the case $b < 0$, uniqueness follows from the uniqueness of the remainder when divided by $-b$: if q, r are unique solutions for the equation $a = q(-b) + r$ with $0 \leq r < b$, then the ones for $a = qb + r$ are unique as well since they differ only by changing the sign of q. □

Problem 4.
Show that $n^5 + 4n$ is divisible by 5 for any integer n.

Proof. Recall that we can write any integer n as $5 \cdot q + r$ for some other integers q, r such that $0 \leq r < 5$. Thus, we can just carry out each of the five cases for each possible remainder to show that the statement is true for every integer:

- $r = 0$, $(5q+0)^5 + 4 \cdot (5q+0) = 5(...) + 0^5 + 4 \cdot 0 = 5(...) + 0$.
- $r = 1$, $(5q+1)^5 + 4 \cdot (5q+1) = 5(...) + 1^5 + 4 \cdot 1 = 5(...) + 5 = 5(...) + 0$
- $r = 2$, $(5q+2)^5 + 4 \cdot (5q+2) = 5(...) + 2^5 + 4 \cdot 2 = 5(...) + 40 = 5(...) + 0$
- $r = 3$, $(5q+3)^5 + 4 \cdot (5q+3) = 5(...) + 3^5 + 4 \cdot 3 = 5(...) + (5+4) \cdot (5+4) \cdot 3 + 12 = 5(...) + 16 \cdot 3 + 12 = 5(...) + 60 = 5(...) + 0$
- $r = 4$, $(5q+4)^5 + 4 \cdot (5q+4) = 5(...) + 4^5 + 4 \cdot 4 = 5(...) + (5 \cdot 3 + 1) \cdot (5 \cdot 3 + 1) \cdot 4 + 16 = 5(...) + 1 \cdot 4 + 16 = 5(...) + 20 = 5(...) + 0$

Thus, since the remainders of all the above numbers when divided by 5 is 0, it is true that $n^5 + 4n$ is divisible by 5 for all integers n. □

Problem 5.
Let x, y, z be integers such that $x^2 + y^2 = z^2$. Show that at least one of x, y, z is divisible by 3.

Proof. Suppose none of them are divisible by 3. Suppose x has remainder 1 when it is being divided by 3, then $x = 3n + 1$ and $x^2 = 9n^2 + 6n + 1 = 3(3n^2 + 2n) + 1$. So x^2 has remainder 1 when being divided by 3. Suppose x has remainder 2 when it is being divided by 3, then $x = 3n + 2$ and $x^2 = 9n^2 + 12n + 4 = 3(9n^2 + 12n + 1) + 1$. So x^2 has remainder 1 when being divided by 3. Similar argument goes for y and z. We can conclude that all of x^2, y^2 and z^2 have remainder 1 when being divided by 3. Suppose $x^2 = 3k + 1$ and $y^2 = 3m + 1$, then $x^2 + y^2 = 3(k + m) + 2$, having remainder 2 when divided by 3. This is a contradiction to $z^2 = x^2 + y^2$ having remainder 1 when divided by 3. So there must be at least one number divisible by 3 among x, y and z. □

Problem 6.
Is it possible to write 1986 as a sum of 6 squares of odd numbers?
Hint: the remainder when divided by 8 yield a contradiction.