Math 255 - Spring 2018
Homework 3 Solutions

1. (a) We have

$$\begin{aligned} 227 &= 143 \cdot 1 + 84 \\ 143 &= 84 \cdot 1 + 59 \\ 84 &= 59 \cdot 1 + 25 \\ 59 &= 25 \cdot 2 + 9 \\ 25 &= 9 \cdot 2 + 7 \\ 9 &= 7 \cdot 1 + 2 \\ 7 &= 2 \cdot 3 + 1 \\ 2 &= 1 \cdot 2 + 0. \end{aligned}$$

The last nonzero remainder is 1, so $(143, 227) = 1$.

(b) We have

$$\begin{aligned} 1479 &= 272 \cdot 5 + 119 \\ 272 &= 119 \cdot 2 + 34 \\ 119 &= 34 \cdot 3 + 17 \\ 34 &= 17 \cdot 2 + 0 \end{aligned}$$

The last nonzero remainder is 17, so $(272, 1479) = 17$.

2. An easy way to prove this fact is to use the Division Algorithm. There are also many other ways, of course.

Let n be an integer. Then by the Division Algorithm, n must either be of the form $n = 3q$, $n = 3q + 1$ or $n = 3q + 2$, where in each case q is an integer. We consider each case in turn.

If $n = 3q$, then $n^2 = (3q)^2 = 9q^2 = 3(3q^2)$. Since $3q^2$ is an integer, n^2 is of the form $3k$ for $k = 3q^2$.

If $n = 3q + 1$, then $n^2 = (3q + 1)^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1$. Since $3q^2 + 2q$ is an integer, n^2 is of the form $3k + 1$ for $k = 3q^2 + 2q$.

Finally, if $n = 3q + 2$, then $n^2 = (3q + 2)^2 = 9q^2 + 12q + 4 = 3(3q^2 + 4q + 1) + 1$. Since $3q^2 + 4q + 1$ is an integer, n^2 is of the form $3k + 1$ for $k = 3q^2 + 4q + 1$.

Therefore, no matter what the remainder of n is when divided by 3, n^2 is of the form $3k$ or $3k + 1$, and the proof is complete.

3. We use the fact that if r is a root of a polynomial, then $x - r$ divides the polynomial. Since $x^2 + ax + b$ is monic and of degree 2, the quotient of $x^2 + ax + b$ by $x - r$ must be monic of degree 1. This implies that there must be some other number t (at this point t could be a complex number) such that

$$x^2 + ax + b = (x - r)(x - t).$$

Expanding the right hand side, we get

$$x^2 + ax + b = x^2 - (r + t)x + rt.$$

Since x^2, x and 1 are linearly independent, this forces the following equalities:

$$a = -(r + t) \quad \text{and} \quad b = rt.$$

Assume that r is the integer root whose existence is guaranteed by hypothesis, and recall that a is an integer as well. Therefore, $t = -(a + r)$ is also an integer. Now since $b = rt$ and t is an integer, it follows that r divides b.

Alternative proof: Let r be the integer root of the polynomial given by the problem. Since r is a root of the polynomial, we have that

$$r^2 + ar + b = 0.$$

Rearranging, we obtain

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

Since both r and a are integers, so is $-r - a$, and therefore r divides b.

4. Since n is an odd integer, there is an integer m such that $n = 2m + 1$. Therefore we have

$$n^2 = (2m + 1)^2 = 4m^2 + 4m + 1 = 1 + 4m(m + 1).$$

If we can prove that $m(m + 1)$ is even, then we will be done. So let's do this.

By the Division Algorithm, m is either of the form $m = 2q$ or of the form $m = 2q + 1$, for q an integer. We consider each case in turn. If $m = 2q$, then $m(m + 1) = 2q(2q + 1) = 2\left(q(2q + 1)\right)$ is even, since $q(2q + 1)$ is an integer. If $m = 2q + 1$, then $m(m+1) = (2q+1)(2q+2) = 2(2q+1)(q+1)$, which is also even, since $(2q+1)(q+1)$ is an integer. Therefore we conclude that in any case, $m(m + 1) = 2k$ for some integer k.

Plugging this into the equation $n^2 = 1 + 4m(m + 1)$, we obtain

$$n^2 = 1 + 4 \cdot 2k = 1 + 8k,$$

where k is an integer, as desired.