Complete Solutions to Exercises 2.3

1. We use Dirichlet's Theorem (2.17):

> Let a and b be *relatively prime* positive integers, then the arithmetic progression $a,\ a+b,\ a+2b,\ a+3b,\ \cdots$contains infinitely many primes.

(a) We are asked to prove there are an infinitely many primes of the form $4n+1$.

Proof.

The form $4n+1$ contains the list of integers:

$$1+4, 1+2\left(4\right), 1+3\left(4\right), \cdots, 1+n\left(4\right),\ \cdots \quad (*)$$

which is an arithmetic progression.

Let $a=1$ and $b=4$ then $\gcd\left(a,\ \ b\right)=1$ so a and b are relatively prime. By Dirichlet's theorem we can say that the list (*) contains infinitely many primes. Hence there are an infinite infinitely many primes of the form $4n+1$.

■

(b) We are asked to prove there are an infinite number of primes of the form $4n+3$.

Proof. Very similar to part (a) but with $a=3$ and $b=4$.

(c) We need to prove that every prime $p>3$ looks like $6n+5$ or $6n+1$.

Proof.

Since $\gcd\left(6,\ \ 5\right)=\gcd\left(6,\ \ 1\right)=1$ so by Dirichlet's theorem $6n+5$ or $6n+1$ contains an infinitely many primes for $n=1, 2, 3, \cdots$.

All the primes greater than 3 are *odd* and *not* multiples of 3. By the Division Algorithm we have for any odd integer a

$$a=6n+1, 6n+3, 6n+5$$

The integer $6n+3=3\left(2n+1\right)$ is a multiple of 3 so *cannot* be prime. Hence all the primes greater than 3 are captured by $6n+5$ or $6n+1$. This completes our proof.

■

2. (a) Again, we use Dirichlet's theorem to prove there are an infinitely many primes of the form $3n+1$.

Proof.

Integers of the form $3n+1$ are

$$1+3, 1+2\big(3\big), 1+3\big(3\big), \cdots, 1+n\big(3\big), \ \cdots$$

Since the $\gcd\big(1, \ \ 3\big)=1$ so by Dirichlet's Theorem (2.17) we conclude that there are infinitely many primes of the form $3n+1$.

■

(b) Similarly, by applying Dirichlet's theorem we can prove there are an infinitely many primes of the form $3n+2$.

(c) Clearly you *cannot* have primes of the form $3n+3$ because $3n+3=3\big(n+1\big)$, so these numbers will have a factor of 3 which implies they are composite.

3. (i) We need to prove that the product of 3 consecutive odd numbers is divisible by 3.

We do this by using proof by induction.

Proof.

Clearly the product $1\times 3\times 5$ is divisible by 3.

Let the three consecutive odd integers be given by:

$$2n+1, \ \ 2n+3, \ \ 2n+5$$

Consider the product $\big(2n+1\big)\big(2n+3\big)\big(2n+5\big)$.

Assume the result is true for $n=k$ that is;

$$3 \ \Big| \ \big(2k+1\big)\big(2k+3\big)\big(2k+5\big) \qquad (*)$$

Required to prove the result for $n=k+1$:

$$3 \ \Big| \ \big(2k+3\big)\big(2k+5\big)\big(2k+7\big)$$

We can rewrite $\big(2k+3\big)\big(2k+5\big)\big(2k+7\big)$ as

$$\begin{aligned}\big(2k+3\big)\big(2k+5\big)\big(2k+7\big) &= \big(2k+3\big)\big(2k+5\big)\big(2k+1+6\big)\\ &= \underbrace{\big(2k+3\big)\big(2k+5\big)\big(2k+1\big)}_{3 \ \Big| \ \big(2k+3\big)\big(2k+5\big)\big(2k+1\big) \text{ by } (*)} + 6\big(2k+3\big)\big(2k+5\big)\\ &= 3m+3\big(2\big)\big(2k+3\big)\big(2k+5\big) \ \text{ where } 3m=\big(2k+3\big)\big(2k+5\big)\big(2k+1\big)\\ &= 3\Big[m+\big(2\big)\big(2k+3\big)\big(2k+5\big)\Big]\end{aligned}$$

Thus $3 \ \Big| \ \big(2k+3\big)\big(2k+5\big)\big(2k+7\big)$. By mathematical induction we have our result that the product of 3 consecutive odd numbers is divisible by 3.

■

(ii)We are asked to prove that $p=3$ is the *only* prime such that p, $p+2$ and $p+4$ are all prime.

Proof.

If $p = 2$ then $p + 2 = 4$ so $p + 2$ is composite.

Clearly it is true for $p = 3$ because 3, 5 and 7 are all prime. *How do we prove that this is the only instance when p, $p + 2$ and $p + 4$ are all prime?*

By contradiction and using the result of part (i).

Suppose $p > 3$ is prime and $p + 2$, $p + 4$ are also prime.

We have p is odd and $p + 2$, $p + 4$ are also odd. By the result of part (i) we have $3 \mid p(p+2)(p+4)$. This is a contradiction because the only factors of p, $p + 2$ and $p + 4$ are 1 and p, $p + 2$ and $p + 4$ respectively and $p > 3$.

This completes our proof.

■

4. (a) We are asked to prove that if a prime is the sum of two squares then it is of the form $4n + 1$.

Proof.

We are given that the prime p is the sum of two squares, so let $p = a^2 + b^2$.

By result of question 2 of Exercises 1.2 we have that the square of any integer is of the form $4m$ or $4m + 1$. Therefore the sum of two squares is

$$a^2 + b^2 = \underbrace{4m_1 + 0, 1}_{=a^2} + \underbrace{4m_2 + 0, 1}_{=b^2} = 4(m_1 + m_2) + 0, 1$$

Clearly $a^2 + b^2 = 4(m_1 + m_2) + 0 = 4(m_1 + m_2)$ *cannot* be prime as 4 is a factor.

The other case $a^2 + b^2 = 4(m_1 + m_2) + 1 = 4n + 1$ may be prime or composite.

Therefore if $a^2 + b^2$ is prime then it has the form $4n + 1$.

■

(b) This time we are asked to prove that a prime of the form $4n + 3$ *cannot* be written as sum of two squares.

Proof.

Let prime $p = 4n + 3$. Suppose this can be written as sum of two squares, that is $a^2 + b^2 = 4n + 3$. By the proof of part (a) we have

$$a^2 + b^2 = 4n + 1$$

Because p is prime. This is a contradiction as $p = 4n + 3$ and the same prime is $p = 4n + 1$.

Thus a prime of the form $4n + 3$ *cannot* be written as sum of two squares.

■