A: There exist primes $p$ such that $p + 6k$ is also prime for $k = 1, 2$ and $3$. One such prime is $p = 11$. Another such prime is $p = 41$. Prove that there exists exactly one prime $p$ such that $p + 6k$ is also prime for $k = 1, 2, 3$ and $4$.

**SOLUTION:** First of all, note that $p = 5$ has the stated property. Indeed,

$$5, \quad 5 + 6 = 11, \quad 5 + 12 = 17, \quad 5 + 18 = 23, \quad 5 + 24 = 29$$

are all prime.

Note that $p = 2$ and $p = 3$ don’t have the stated property. Now let us consider a prime $p > 5$. We can write $p = 5q + r$, where $r \in \{0, 1, 2, 3, 4\}$. We will consider each of the five cases separately. Since $p > 5$, we have $q \geq 1$.

Case 1: Assume $r = 0$. Then $p = 5q$ and hence $5 \mid p$. Since $p > 5$, we have $q > 1$ in this case. This is impossible because $p$ is a prime.

Case 2: Assume $r = 1$. Then $p + 24 = (5q + 1) + 24 = 5q + 25 = 5(q + 5)$. Since $q + 5 > 1$, it follows that $p + 24$ is not prime.

Case 3: Assume $r = 2$. Then $p + 18 = (5q + 2) + 18 = 5q + 20 = 5(q + 4)$. Since $q + 4 > 1$, it follows that $p + 18$ is not prime.

Case 4: Assume $r = 3$. Then $p + 12 = (5q + 3) + 12 = 5q + 15 = 5(q + 3)$. Since $q + 3 > 1$, it follows that $p + 12$ is not prime.

Case 5: Assume $r = 4$. Then $p + 6 = (5q + 4) + 6 = 5q + 10 = 5(q + 2)$. Since $q + 2 > 1$, it follows that $p + 6$ is not prime.

In summary, if $p > 5$, then we have shown that at least one of the numbers

$$p, \quad p + 6, \quad p + 12, \quad p + 18, \quad p + 24$$

is not prime. We have also ruled out $p = 2$ and $p = 3$. It follows that exactly one prime $p$ has the stated property, namely $p = 5$.

B: Prove that if $n \in \mathbb{Z}$, then $n^3$ gives a remainder of $0, 1$, or $6$ when divided by $7$. 

1
**SOLUTION:** By the Division Algorithm, we know that \( n = 7q + r \), where \( r \in \{0, 1, 2, 3, 4, 5, 6\} \). We will consider all seven cases separately. First note that

\[
n^3 = (7q + r)^3 = (7q)^3 + 3(7q)^2r + 3(7q)r^2 + r^3 = 7(7^2q^3 + 3 \cdot 7q^2r + 3qr^2) + r^3.
\]

Thus, \( n^3 = 7k + r^3 \), where \( k = 7^2q^3 + 3 \cdot 7q^2r + 3qr^2 \). Since \( q \) and \( r \) are in \( \mathbb{Z} \), it follows that \( k \in \mathbb{Z} \).

Now we consider the seven cases. Note that

\[
0^3 = 0 = 7 \cdot 0 + 0, \quad 1^3 = 1 = 7 \cdot 0 + 1, \quad 2^3 = 8 = 7 \cdot 1 + 1, \quad 3^3 = 27 = 7 \cdot 3 + 6, \\
4^3 = 64 = 7 \cdot 9 + 1, \quad 5^3 = 125 = 7 \cdot 17 + 6, \quad 6^3 = 216 = 7 \cdot 30 + 6.
\]

In each case, we have found that \( r^3 = 7u + v \), where \( u \in \mathbb{Z} \) and \( v \in \{0, 1, 6\} \).

Finally, we have \( n^3 = 7k + r^3 = 7k + 7u + v = 7(k + u) + v \), where \( v \in \{0, 1, 6\} \). Note that \( k + u \in \mathbb{Z} \). It follows that the remainder that \( n^3 \) gives when divided by 7 is either 0 or 1 or 6.

C: Prove that if \( n \) is an odd integer, then \( n \) is of the form \( 4k + 1 \) or \( 4k + 3 \), where \( k \in \mathbb{Z} \).

**SOLUTION:** Since \( n \) is an integer, by the Division Algorithm, we have \( n = 4k + r \), where \( k \in \mathbb{Z} \) and \( r \in \{0, 1, 2, 3\} \). If \( r = 0 \), then \( n = 4q = 2(2q) \) is even. If \( r = 2 \), then \( n = 4q + 2 = 2(2q + 1) \) and \( n \) is also even in this case. Thus, if \( n \) is odd, then \( r \neq 0 \) and \( r \neq 2 \). It follows that if \( n \) is odd, then \( r = 1 \) or \( r = 3 \). Thus, if \( n \) is odd, we must have \( n = 4k + 1 \) or \( n = 4k + 3 \), where \( k \in \mathbb{Z} \).

D: Prove that if \( n \) is an odd integer, then \( n^2 \) gives a remainder of 1 when divided by 8.

**SOLUTION:** We will use the result from problem C. Assume that \( n \) is odd. Then we know that \( n = 4k + 1 \) or \( n = 4k + 3 \), where \( k \in \mathbb{Z} \).

If \( n = 4k + 1 \), then \( n^2 = (4k + 1)^2 = 16k^2 + 8k + 1 = 8(2k^2 + 1) + 1 \). Since \( 2k^2 + 1 \) is an integer, it follows that \( n^2 \) gives a remainder of 1 when divided by 8.

If \( n = 4k + 3 \), then \( n^2 = (4k + 3)^2 = 16k^2 + 24k + 9 = 8(2k^2 + 3k + 1) + 1 \). Since \( 2k^2 + 3k + 1 \) is an integer, it follows that \( n^2 \) gives a remainder of 1 when divided by 8.

In summary, if \( n \) is odd, then \( n^2 \) gives a remainder of 1 when divided by 8.
E: Prove that if \( n \) is an even integer, then \( n^2 \) gives a remainder of 0 or 4 when divided by 8.

**SOLUTION:** Suppose that \( n \) is even. Then \( n = 2k \), where \( k \in \mathbb{Z} \). Hence \( n^2 = 4k^2 \) and hence \( n^2 \) is divisible by 4. Thus, we have \( 4 \mid n^2 \).

By the Division Algorithm, we have \( n^2 = 8q + r \), where \( r \in \{0, 1, 2, 3, 4, 5, 6, 7\} \) and \( q \in \mathbb{Z} \). We have \( r = n^2 - 8q \). Note that \( 8q = 4(2q) \) is divisible by 4. Since \( 4 \mid n^2 \) and \( 4 \mid 8q \), it follows that \( 4 \mid (n^2 - 8q) \). Thus, we must have \( 4 \mid r \). Since, \( r \in \{0, 1, 2, 3, 4, 5, 6, 7\} \), it follows that either \( r = 0 \) or \( r = 4 \). Hence, \( n^2 \) indeed gives a remainder of 0 or 4 when \( n \) is even.

F: Do problem 6 on page 25.

6(a) **SOLUTION:** We have

\[
\begin{align*}
12075 &= 4655 \cdot 2 + 2765 \\
4655 &= 2765 \cdot 1 + 1890 \\
2765 &= 1890 \cdot 1 + 875 \\
1890 &= 875 \cdot 2 + 140 \\
875 &= 140 \cdot 6 + 35 \\
140 &= 35 \cdot 4 + 0
\end{align*}
\]

and so we can conclude that \((4655, 12075) = 35\). Using the above equations, we find

\[
\begin{align*}
35 &= 875 - 6 \cdot 140 = 875 - 6 \cdot (1890 - 2 \cdot 875) = 13 \cdot 875 - 6 \cdot 1890 = 13 \cdot (2765 - 1 \cdot 1890) - 6 \cdot 1890 \\
&= 13 \cdot 2765 - 19 \cdot 1890 = 13 \cdot 2765 - 19 \cdot (4655 - 1 \cdot 2765) = 32 \cdot 2765 - 19 \cdot 4655 \\
&= 32 \cdot (12075 - 2 \cdot 4655) - 19 \cdot 4655 = 32 \cdot 12075 - 83 \cdot 4655 .
\end{align*}
\]

We have \(35 = -83 \cdot 4655 + 32 \cdot 12075\) and so we can take \(x = -83\) and \(y = 32\).

6 (b) **SOLUTION:** We have

\[
\begin{align*}
2597 &= 1369 \cdot 1 + 1228 \\
1369 &= 1228 \cdot 1 + 141 \\
1228 &= 141 \cdot 8 + 100 \\
141 &= 100 \cdot 1 + 41
\end{align*}
\]

3
100 = 41 \cdot 2 + 18
41 = 18 \cdot 2 + 5
18 = 5 \cdot 3 + 3
5 = 3 \cdot 1 + 2
3 = 2 \cdot 1 + 1
2 = 1 \cdot 2 + 0

and so we can conclude that \((1369, 2597) = 1.\) Using the above equations, we have

\[
1 = 3 - 1 \cdot 2 = 3 - 1 \cdot (5 - 1 \cdot 3) = 2 \cdot 3 - 1 \cdot 5 = 2 \cdot (18 - 3 \cdot 5) - 1 \cdot 5
\]

\[
= 2 \cdot 18 - 7 \cdot 5 = 2 \cdot 18 - 7 \cdot (41 - 2 \cdot 18) = 16 \cdot 18 - 7 \cdot 41 = 16 \cdot (100 - 2 \cdot 41) - 7 \cdot 41
\]

\[
= 16 \cdot 100 - 39 \cdot 41 = 16 \cdot 100 - 39 \cdot (141 - 1 \cdot 100) = 55 \cdot 100 - 39 \cdot 141 = 55 \cdot 1228 - 8 \cdot 141) - 39 \cdot 141
\]

\[
= 55 \cdot 1228 - 479 \cdot 141 = 55 \cdot 1228 - 479 \cdot (1369 - 1 \cdot 1228) = 534 \cdot 1228 - 479 \cdot 1369
\]

and so we have \(1369 \cdot (−1013) + 2597 \cdot 534 = 1.\) We can take \(x = -1013\) and \(y = 534.\)

6 (c) \quad \textbf{SOLUTION:} We have

\[
2048 = 1275 \cdot 1 + 773
\]

\[
1275 = 773 \cdot 1 + 502
\]

\[
773 = 502 \cdot 1 + 271
\]

\[
502 = 271 \cdot 1 + 231
\]

\[
271 = 231 \cdot 1 + 40
\]

\[
231 = 40 \cdot 5 + 31
\]

\[
40 = 31 \cdot 1 + 9
\]

\[
31 = 9 \cdot 3 + 4
\]

\[
9 = 4 \cdot 2 + 1
\]

\[
4 = 1 \cdot 4 + 0
\]

and so we have \((2048, 1275) = 1.\) Using the above equations, we obtain

\[
1 = 9 - 2 \cdot 4 = 9 - 2 \cdot (31 - 3 \cdot 9) = 7 \cdot 9 - 2 \cdot 31 = 7 \cdot (40 - 1 \cdot 31) - 2 \cdot 31
\]
\[ x^2 - 6y^2 = 10. \]

G: Consider the equation \( x^2 - 6y^2 = 10 \). It turns out that this equation has infinitely many solutions where \( x, y \in \mathbb{Z} \). Suppose that \( x = a, y = b \) is one of those solutions. Prove that \( (a, b) = 1 \).

**SOLUTION:** Let \( d = (a, b) \). In general, we know that \( d \geq 1 \). We will prove that \( d = 1 \).

First of all, note that \( d \mid a \) and \( d \mid b \). This follows from the definition of \( (a, b) \). Thus, we have \( a = de \) and \( b = df \), where \( e, f \in \mathbb{Z} \).

We are given that \( x = a \) and \( y = b \) satisfy the equation \( x^2 - 6y^2 = 10 \). That is, we can assume that \( a^2 - 6b^2 = 10 \). We will now combine this fact with the facts that \( a = de \) and \( b = df \). We obtain the equation \( (de)^2 - 6(df)^2 = 10 \). Equivalently, we have \( d^2 e^2 - 6d^2 f^2 = 10 \). This gives the equation

\[ d^2 (e^2 - 6f^2) = 10. \]

Let \( q = e^2 - 6f^2 \). Since \( e, f \in \mathbb{Z} \), it follows that \( q \in \mathbb{Z} \). Therefore, \( 10 = d^2 q \) and hence we can conclude that \( d^2 \) divides 10.

The divisors of 10 are easily found. They are \( \pm 1, \pm 2, \pm 5, \) and \( \pm 10 \). Only one of these divisors is equal to the square of an integer, namely 1. Therefore, we must have \( d^2 = 1 \). Since \( d \geq 1 \), we must have \( d = 1 \). This is what we wanted to prove.