1. (a) The Euclidean algorithm produces the following steps:

\[
\begin{align*}
13 &= 8 + 5 \\
8 &= 5 + 3 \\
5 &= 3 + 2 \\
3 &= 2 + 1
\end{align*}
\]

so the greatest common divisor is 1. Working backwards yields

\[
\begin{align*}
1 &= 3 - 2 \\
&= 3 - (5 - 3) \\
&= 2(3) - 5 \\
&= 2(8 - 5) - 5 \\
&= 2(8) - 3(5) \\
&= 2(8) - 3(13 - 8) \\
&= 5(8) - 3(13)
\end{align*}
\]

yielding the integer linear combination

\[
1 = (-3)(13) + 5(8) .
\]

(b) The Euclidean algorithm produces the following steps:

\[
\begin{align*}
27 &= 21 + 6 \\
21 &= 3(6) + 3
\end{align*}
\]

so the greatest common divisor is 3. Working backwards yields

\[
\begin{align*}
3 &= 21 - 3(6) \\
&= 21 - 3(27 - 21) \\
&= 4(21) - 3(27)
\end{align*}
\]

yielding the integer linear combination

\[
3 = (-3)(27) + 4(21) .
\]
(c) The Euclidean algorithm produces the following steps:

\[
\begin{align*}
64 &= 2(25) + 14 \\
25 &= 14 + 11 \\
14 &= 11 + 3 \\
11 &= 3(3) + 2 \\
3 &= 2 + 1 \\
\end{align*}
\]

so the greatest common divisor is 1. Working backwards yields

\[
1 = 3 - 2 \\
= 3 - (11 - 3(3)) \\
= 4(3) - 11 \\
= 4(14 - 11) - 11 \\
= 4(14) - 5(11) \\
= 4(14) - 5(25 - 14) \\
= 9(14) - 5(25) \\
= 9(64 - 2(25)) - 5(25) \\
= 9(64) - 23(25) \\
\]

yielding the integer linear combination

\[
1 = 9(64) + (-23)(25) .
\]

(d) The Euclidean algorithm produces the following steps:

\[
\begin{align*}
2^{20} &= 2621(20^2) + 176 \\
20^2 &= 2(176) + 48 \\
176 &= 3(48) + 32 \\
48 &= 32 + 16 \\
\end{align*}
\]

so the greatest common divisor is 16. Working backwards yields

\[
16 = 48 - 32 \\
= 48 - (176 - 3(48)) \\
= 4(48) - 176 \\
= 4(20^2 - 2(176)) - 176 \\
= 4(20^2) - 9(176) \\
= 4(20^2) - 9(2^{20} - 2621(20^2)) \\
= 23,593(20^2) - 9(2^{20}) \\
\]

yielding the integer linear combination

\[
1 = (−9)(2^{20}) + 23,593(20^2) .
\]
2. We sieve out all multiples of primes up to \( \sqrt{100} = 10 \), so remove all multiples of 2, 3, 5 and 7 leaving all primes less than 100:

\[
\]

3. Certainly if \( N \) has a divisor \( M \) such that \( 1 < M \leq \sqrt{N} \) then \( 1 < M < N \) so that \( N \) is composite. Suppose on the other hand that \( N \) is composite. Then \( N = ab \) for some integers \( a \) and \( b \) where \( 1 < a, b < N \). If \( a > \sqrt{N} \) and \( b > \sqrt{N} \) then

\[
N = ab > (\sqrt{N})^2 = N,
\]

which is impossible. Hence \( a \leq \sqrt{N} \) or \( b \leq \sqrt{N} \). This proves \( N \) has at least one nontrivial divisor \( \leq \sqrt{N} \).

4. (a) \( 1,000,000 = 10^6 = (2 \times 5)^6 = 2^6 \cdot 5^6 \).
   
   (b) \( 576,000 = 3 \times 192 \times 10^3 = 3 \times 32 \times 6 \times 2^3 \times 5^3 = 2^9 \cdot 3^2 \cdot 5^3 \).
   
   (c) \( 100^2 - 98^2 = (100 + 98)(100 - 98) = 198 \times 2 = 99 \times 2^2 = 2^2 \cdot 3^2 \cdot 11^1 \).

5. We calculate

\[
100^{100} = 2^{100} \pmod{7} = (2^3)^{33} \times 2 = 1^{33} \times 2 \pmod{7} = 2,
\]

so that, after \( 100^{100} \) days have elapsed, it will be 2 days after a Monday, which is a Wednesday.

*6. Observe first that

\[
(-8)^2 = 64 = -8 \pmod{24}
\]

from which it follows immediately that \(-8\) coincides with all of its positive powers modulo 24. Thus

\[
100^{100} = 4^{100} \pmod{24} = (4^2)^{50} = (-8)^{50} \pmod{24} = -8 \pmod{24} = 16 \pmod{24},
\]

so that, after \( 100^{100} \) hours have elapsed, it will be 16 hours after some 9 a.m., which is 1 a.m. the following day. Thus \( 100^{100} - 16 \) is a multiple of 24, so the number of days is

\[
\frac{100^{100} - 16}{24} = \frac{2 - 2}{3} = 0 \pmod{7}.
\]
Thus after $100^{100} - 16$ hours have elapsed it will again be 9 a.m. on a Monday, so that the meteor strike will be at 1 a.m. on the following Tuesday.

7. (a) The addition and multiplication tables for $\mathbb{Z}_6$ are

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>\cdot</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

(b) If one ignores the last row and column of the multiplication table, one sees that 5 is absent from the body of the remaining table, so that the set $\mathbb{Z}_6 \setminus \{5\} = \{0, 1, 2, 3, 4\}$ is closed under multiplication.

*(c) Denote by $\overline{m}$ the remainder after dividing an integer $m$ by 6. Suppose $a, b \in \mathbb{Z}$ such that $ab = -1 \pmod{6}$. If $a \neq -1 \pmod{6}$ and $b \neq -1 \pmod{6}$ then $\overline{a} \neq 5$ and $\overline{b} \neq 5$, so, by (b),

$$ab = \overline{a} \overline{b} \neq 5 \pmod{6}$$

which contradicts that $ab = -1 \pmod{6}$. Hence

$$a = -1 \pmod{6} \quad \text{or} \quad b = -1 \pmod{6}.$$

Now consider any integer $n \geq 2$ such that $n = -1 \pmod{6}$. By iterating the previous observation, as we successively factorize $n$, we find at least one prime factor $p$ such that $p = -1 \pmod{6}$.

*8. Certainly $p$ is odd, so $p + 1$ is even and divisible by 2. But $p(p + 1)(p + 2)$ is a product of 3 consecutive integers, so must be divisible by the prime 3. Hence 3 divides $p$, $p + 1$ or $p + 2$. However $p$ and $p + 2$ are primes $> 3$ so cannot be divisible by 3. We conclude that $p + 1$ is divisible by 3 also. Hence $p + 1 = p - (-1)$ is divisible by $3 \times 2 = 6$, which proves $p = -1 \pmod{6}$.

**9.** Suppose there are finitely many primes $p_1, \ldots, p_m$ equal to $-1$ modulo 6. Put

$$n = \begin{cases} (p_1 \times \cdots \times p_m) + 4 & \text{if } m \text{ is even} \\ (p_1 \times \cdots \times p_m) + 6 & \text{if } m \text{ is odd} \end{cases}$$

so in either case $n = -1 \pmod{6}$. By 7(c), $n$ has a prime divisor $p = -1 \pmod{6}$. But $p \in \{p_1, \ldots, p_m\}$, so, from the definition of $n$, either $p \mid 4$ or $p \mid 6$, whence $p = 2 \neq -1 \pmod{6}$ or $p = 3 \neq -1 \pmod{6}$, a contradiction. Hence there are infinitely many primes equal to $-1$ modulo 6.
10. Let \( N \) be any positive integer. Since there are infinitely many primes, choose a prime \( p \geq N + 2 \). List all the primes less than or equal to \( p \):

\[
p_1 < p_2 < \ldots < p_M < p.
\]

Note that \( M \geq 1 \). Put

\[
Q = p_1 \times \ldots \times p_M
\]

and let

\[
X = \{ z \in \mathbb{Z} \mid Q + 2 \leq z \leq Q + p - 1 \}.
\]

Thus \( X \) consists of consecutive integers and has size \( p - 2 \geq N \). Consider any \( z \in X \). Then

\[
2 \leq z - Q \leq p - 1 < p
\]

so that \( z - Q \) is a product of primes smaller than \( p \). Hence \( p_i \) divides \( z - Q \) for some \( i \leq M \). But \( p_i \) also divides \( Q \), so \( p_i \) divides \( z - Q + Q = z \). This proves every element of \( X \) is composite.