Contents

1 1

Use the Euclidean Algorithm to find $\gcd(7544, 115)$. Then express the greatest common divisor as a linear combination of 7544 and 115.

$$
\begin{aligned}
7544 &= 65 \cdot 115 + 69 \\
115 &= 1 \cdot 69 + 46 \\
69 &= 1 \cdot 46 + 23 \\
46 &= 2 \cdot 23 + 0 \\
\therefore \gcd(7544, 115) &= 23
\end{aligned}
$$

$$
\begin{aligned}
&23 = 69 - 1 \cdot 46 \\
&46 = 115 - 1 \cdot 69 \\
&23 = 69 - 1 \cdot (115 - 1 \cdot 69) \\
&23 = 2 \cdot 69 - 1 \cdot 115 \\
&69 = 7544 - 65 \cdot 115 \\
&23 = 2(7544 - 65 \cdot 115) - 1 \cdot 115 \\
&23 = 2 \cdot 7544 - 131 \cdot 115
\end{aligned}
$$

2 2

Find an inverse of a modulo m by Euclidean Algorithm, where $a = 74, m = 389$.

$$
\begin{aligned}
389 &= 5 \cdot 74 + 19 \\
74 &= 3 \cdot 19 + 17 \\
19 &= 1 \cdot 17 + 2 \\
17 &= 8 \cdot 2 + 1 \\
2 &= 2 \cdot 1 \\
\therefore \gcd(74, 389) &= 1
\end{aligned}
$$

$$
\begin{aligned}
1 &= 17 - 8 \cdot 2 \\
2 &= 19 - 1 \cdot 17 \\
1 &= 17 - 8 \cdot (19 - 1 \cdot 17) \\
1 &= 9 \cdot 17 - 8 \cdot 19 \\
17 &= 74 - 3 \cdot 19 \\
1 &= 9 \cdot (74 - 3 \cdot 19) - 8 \cdot 19 \\
1 &= 9 \cdot 74 - 35 \cdot 19 \\
19 &= 389 - 5 \cdot 74 \\
1 &= 9 \cdot 74 - 35 \cdot (389 - 5 \cdot 74) \\
1 &= 184 \cdot 74 - 35 \cdot 389
\end{aligned}
$$

$$
\begin{aligned}
sa + tm &= 1(\bmod(m)) \\
184 \cdot 74 - 35 \cdot 389 &\equiv 1(\bmod(389)) \\
184 \cdot 74 &\equiv 1(\bmod(389))
\end{aligned}
$$

184 is an inverse of a mod (m).

3 3

Solve the congruence $74x \equiv 5(\bmod(389))$ using the modular inverse from the previous problem.

$$
\begin{aligned}
184 \cdot [74x] &\equiv [5(\bmod(389))] \cdot 184 \\
x &\equiv 142(\bmod(389))
\end{aligned}
$$

4 4

Show that if $ac \equiv bc(\bmod(m))$, where a, b, c, and m are integers with $m > 2$, and $d = \gcd(m, c)$, then $a \equiv b \left(\bmod\left(\frac{m}{d}\right)\right)$.

$$
\begin{aligned}
ac \equiv bc(\bmod(m)) &\iff m \mid ac - bc \\
ac - bc &= k \cdot m \\
a\left(d \cdot \frac{c}{d}\right) - b\left(d \cdot \frac{c}{d}\right) &= k\left(d \cdot \frac{m}{d}\right) \\
a\left(\frac{c}{d}\right) - b\left(\frac{c}{d}\right) &= k\left(\frac{m}{d}\right) \\
a\left(\frac{c}{d}\right) &\equiv b\left(\frac{c}{d}\right) \bmod \left(\frac{m}{d}\right) \\
a &\equiv b \bmod \left(\frac{m}{d}\right)
\end{aligned}
$$