Mathematics 216
Robert Gross
Homework 21
Answers

1. Suppose that $f : X \to Y$, and that f is an injection. Prove that for every set $A \subset X$, $f^{-1}(f(A)) = A$.

Answer: Pick a subset $A \subset X$. Suppose first that $a \in A$. Then $f(a) \in f(A)$, and by definition, that means that $a \in f^{-1}(f(A))$. Note that this part of the argument does not require f to be an injection.

Now, suppose that $b \in f^{-1}(f(A))$. This means that $f(b) \in f(A)$, and therefore there is some element $a \in A$ so that $f(b) = f(a)$. But f is injective, so we can conclude that $b = a$, and therefore $b \in A$.

2. Use the Euclidean algorithm to solve the congruence

$$32y \equiv 11 \pmod{107}.$$

Answer: We start with division:

$$\begin{aligned} 107 &= 3 \cdot 32 + 11 \\ 32 &= 2 \cdot 11 + 10 \\ 11 &= 1 \cdot 10 + \ \ 1 \end{aligned}$$

Therefore,

$$\begin{aligned} 1 &= 1 \cdot 11 &&+ (-1) \cdot (10) \\ &= 1 \cdot 11 &&+ (-1) \cdot (32 - 2 \cdot 11) \\ &= 3 \cdot 11 &&+ (-1) \cdot (32) \\ &= 3 \cdot (107 - 3 \cdot 32) &&+ (-1) \cdot (32) \\ &= 3 \cdot 107 &&+ (-10) \cdot (32) \end{aligned}$$

So we now know that $(32)(-10) \equiv 1 \pmod{107}$. Multiplying by 11, we have $23(-10 \cdot 11) \equiv 11 \pmod{107}$. So one possible solution for x would be $-10 \cdot 11 = -110$, but it is kinder to notice that $-110 \equiv -3 \equiv 104 \pmod{107}$, and take $x \equiv 104 \pmod{107}$.

3. Suppose that the congruence $ax \equiv b \pmod{n}$ has at least one solution. Show that $(a, n) | b$.

Answer: If the congruence $ax \equiv b \pmod{n}$ has a solution, then we know that for some value of x, $n | ax - b$. Equivalently, we can write $nq = ax - b$, or $b = ax - nq$. We know that $(a, n) | a$ and $(a, n) | n$, so elementary properties of divisibility tell us that $(a, n) | b$.