Math 55, Solutions to In-class Problems
Feb 12, 2013

1. Problem: prove that if $a \equiv b \mod m$ where $a, b, m \in \mathbb{Z}$ and $m \geq 2$ then $\gcd(a, m) = \gcd(b, m)$.

   Solution: We will show that $\gcd(b, m)$ divides $\gcd(a, m)$. By symmetry, we will have also shown that $\gcd(a, m)$ divides $\gcd(b, m)$. Thus we will have shown that $\gcd(a, m) = \gcd(b, m)$.

   Let $a \equiv b \mod m$. Then there exists an integer k such that $a = b + km$. For any integer x such that x divides m and x divides b (i.e. x divides $\gcd(b, m)$), we see that x divides a. Indeed, if we write $b = b_0 x$ and $m = m_0 x$ then $a = b_0 x + k m_0 x = x(b_0 + k m_0)$. Since this is true for any divisor of $\gcd(b, m)$, we conclude that $\gcd(b, m)$ divides a. But by definition, $\gcd(b, m)$ divides m. Thus $\gcd(b, m)$ divides $\gcd(a, m)$.

2. Prove that there is a composite integer in any arithmetic progression $b + a, b + 2a, b + 3a, b + 4a, \ldots$ where a and b are positive integers.

   Solution: The b^{th} term of this sequence is $b + ba = b(1 + a)$. Since $a \in \mathbb{Z}_+$, we have $a \geq 1$, so $a + 1 \geq 2$. Thus for any arithmetic progression with $b > 1$, the b^{th} term is a product of two positive integers not equal to 1 and therefore composite.

   It remains to show that an arithmetic progression of the form

   $$1 + a, 1 + 2a, 1 + 3a, 1 + 4a, \ldots$$

   has a composite term. Note that $(a+1)^2 = a^2 + 2a + 1 = a(a+2) + 1$. So the $(a+2)^{\text{th}}$ term of the sequence, $a(a+2)+1$, is the square of the integer $a + 1$. We saw above that $a + 1 \geq 2$, so the $(a + 2)^{\text{th}}$ term is composite.

   Thus we see that for any arithmetic progression $b+a, b+2a, b+3a, b+4a, \ldots$, there is a composite term in either the b^{th} place or the $(a+2)^{\text{th}}$ place.

3. Prove that if $m > 1$ and

$$ac \equiv bc \mod m$$

then

$$a \equiv b \mod m/\gcd(c, m).$$

Solution: Let $ac \equiv bc \mod m$. Then by definition, there exists and integer k such that $ac = bc + km$. Let $x := \gcd(c, m)$, and write $m = m_0 x$ and $c = c_0 x$. Then

$$ac_0 x = bc_0 x + km_0 x$$

so

$$ac_0 = bc_0 + km_0.$$

By the definition of gcd, c_0 and m_0 are relatively prime (indeed, if they had a common divisor $y \neq 1$ then y would divide both c and m, so xy would divide both c and m, but we defined x to be the greatest integer dividing both c and m). Thus there exists an integer c_0^{-1} such that $c_0 \cdot c_0^{-1} \equiv 1 \mod m_0$. Multiplying both sides of the above equation by c_0^{-1} yields

$$acc_0^{-1} = bcc_0^{-1} + km_0 c_0^{-1}.$$

Take both sides of the above equality $\mod m_0$ and we have

$$acc_0^{-1} \equiv bcc_0^{-1} + km_0 c_0^{-1} \mod m_0$$

so

$$acc_0^{-1} \equiv bcc_0^{-1} \mod m_0$$

so

$$a \equiv b \mod m_0.$$