

MATH 567 FALL 2008, NUMBER THEORY I, SOLUTIONS 2

1. Let $a, b, c \in \mathbb{Z}$ with a and b not both zero. Prove each of the following. (i) If $(a, b) = 1$ and $a|bc$, then $a|c$. (ii) $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$. (iii) $(a, b) = (a + cb, b)$. (i) There are x and y such that $ax + by = 1$. Thus $acx + bcy = c$ and $a|bc$ so $a|acx + bcy$. (ii) There are x and y such that $ax + by = 1$. Since $(a, b)|a$, $(a, b)|b$ and so $\frac{a}{(a,b)}x + \frac{b}{(a,b)}y = 1$. Hence $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) | 1$. (iii) There are x and y such that $ax + by = (a, b)$. Thus $(a, b)|(a + bc, b)|(a + bc)x + b(y - cx) = ax + by = (a, b)$.
2. Show that if $(a, b) = 1$, then $(a - b, a + b) = 1$ or 2 . Exactly when is the value 2 ? We have $(a - b, a + b) = (2a, a + b)|(2a, 2a + 2b) = (2a, 2b) = 2(a, b) = 2$. For equality in this, $(2a, a + b) = 2$. This holds iff $2|a + b$. But $(a, b) = 1$. Hence $(a - b, a + b) = 2$ iff a and b are both odd.
3. Show that if $(b, c) = 1$, then $(a, bc) = (a, b)(a, c)$, and that $(bx + cy, bc) = (b, y)(c, x)$ for all integers x and y . Let $a = \pm \prod_p p^{\alpha_p}$, $b = \pm \prod_p p^{\beta_p}$, $c = \pm \prod_p p^{\gamma_p}$ be the canonical decompositions, where $\alpha_p \geq 0$, $\beta_p \geq 0$, $\gamma_p \geq 0$. Then $(b, c) = 1$ iff $\beta_p \gamma_p = 0$. Thus $\min(\alpha_p, \beta_p + \gamma_p) = \min(\alpha_p, \beta_p) + \min(\alpha_p, \gamma_p)$. $(bx + cy, bc) = (bx + cy, b)(bx + cy, c) = (cy, b)(bx, c) = (y, b)(x, c)$.
4. Find integers x and y such that $525x + 231y = (525, 231)$. $525 = 231 \cdot 2 + 63$, $231 = 63 \cdot 3 + 42$, $63 = 42 \cdot 1 + 21$, $42 = 21 \cdot 2$. $21 = 63 - 42 = 63 - (231 - 63 \cdot 3) = 4(525 - 231 \cdot 2) - 231 = 525 \cdot 4 - 231 \cdot 9$.
5. Show that if $ad - bc = \pm 1$, then $(a + b, c + d) = 1$. We have $(a + b)d - (c + d)b = \pm 1 + bd - bd = \pm 1$.
6. (L. Mirsky and D. J. Newman) Suppose that $K \geq 2$, $0 \leq a_k < m_k$ for $1 \leq k \leq K$ and that $m_1 < m_2 < \dots < m_K$. This is called a *family of covering congruences* when every integer x satisfies at least one of the congruences $x \equiv a_k \pmod{m_k}$. A system of covering congruences is called *exact* when for every value of x there is exactly one value of k such that $x \equiv a_k \pmod{m_k}$. Show that if the system is exact, then

$$\sum_{k=1}^K \frac{z^{a_k}}{1 - z^{m_k}} = \frac{1}{1 - z}.$$

Let $e(\alpha)$ denote $e^{2\pi i \alpha}$ where $i = \sqrt{-1}$. When $z = re(1/m_K)$ with $r \in \mathbb{R}_{>0}$ and $r \rightarrow 1-$, show that the left hand side above is

$$\sim \frac{e(a_K/m_K)}{m_K(1 - r)}$$

whereas the right hand side is bounded for z in a neighbourhood of $e(1/m_K)$.

We have

$$\sum_{n=0}^{\infty} z^n = \sum_{k=1}^K \sum_{n=0}^{\infty} z^{nm_k + a_k}$$

when $|z| < 1$. LHS is $\frac{1}{1-z}$. RHS is $\sum_{k=1}^K \frac{z^{a_k}}{1 - z^{m_k}}$. When $z = re^{2\pi i/m_K}$ we have $z \rightarrow e^{2\pi i/m_K} \neq 1$ as $r \rightarrow 1-$, so $\lim_{r \rightarrow 1-} \frac{1}{1-z}$ exists. When $k < K$, $z^{m_k} = r^{m_k} e^{2\pi i m_k/m_K} \rightarrow e^{2\pi i m_k/m_K} \neq 1$ as $r \rightarrow 1-$, so the terms on the RHS with $k < K$ also converge. On the other hand

$$\frac{z^{a_K}}{1 - z^{m_K}} = \frac{r^{a_K} e^{2\pi i a_K/m_K}}{1 - r^{m_K}} \sim \frac{e^{2\pi i a_K/m_K}}{m_K(1 - r)}$$

which diverges.