Math 3063 Abstract Algebra Project 1 **Solutions**
Prof. Paul Bailey March 2, 2009

Problem 1. Use induction to prove that, for all $n \in \mathbb{N}$,

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}.$$

Solution. For $n = 1$, we have

$$\sum_{i=1}^{n} i^2 = 1^2 = 1 = \frac{1(1+1)(2+1)}{6}.$$

Let $n > 1$. By induction,

$$\sum_{i=1}^{n-1} i^2 = \frac{(n-1)n(2(n-1)+1)}{6}.$$

Adding n^2 to both sides gives

$$\begin{aligned}\sum_{i=1}^{n} i^2 &= \frac{(n-1)n(2(n-1)+1)}{6} + n^2 \\ &= \frac{(n^2-n)(2n-1)}{6} + \frac{6n^2}{6} \\ &= \frac{(2n^3-3n^2+n)+6n^2}{6} \\ &= \frac{2n^3+3n^2+n}{6} \\ &= \frac{n(n+1)(2n+1)}{6}.\end{aligned}$$

□

Problem 2. Let $m = 71$ and $n = 528$. Find $x, y, d \in \mathbb{Z}$ such that $mx + ny = d$ and $d = \gcd(m, n)$.

Solution. We apply the Euclidean algorithm to find that

$$\begin{aligned}528 &= 71(7) + 31 \\ 71 &= 31(2) + 9 \\ 31 &= 9(3) + 4 \\ 9 &= 4(2) + 1\end{aligned}$$

Thus $\gcd(71, 528) = 1$. Rewinding, we find that

$$\begin{aligned}1 &= 4(-2) + 9 \\ &= 9(7) + 31(-2) \\ &= (31(-16) + 71(7) \\ &= 71(119) + 528(-16)\end{aligned}$$

Let $d = 1$, $x = 119$, and $y = -16$. Then $mx + ny = d$. □

Problem 3. Let $a, b, c \in \mathbb{Z}$ be positive integers. Show that

(a) $a \mid a$;

(b) $a \mid b$ and $b \mid a$ implies $a = b$;

(c) $a \mid b$ and $b \mid c$ implies $a \mid c$.

Solution.

(a) (Reflexivity) Since $a = 1 \cdot a$, $a \mid a$.

(b) (Antisymmetry) Suppose $a \mid b$ and $b \mid a$. Then $b = ma$ and $a = nb$ for some $m, n \in \mathbb{Z}$. Thus $b = mnb$, and by cancelation, we have $mn = 1$. Thus $m = n = \pm 1$. Since a and b are positive, we must have $m = n = 1$, so $a = b$.

(c) (Transitivity) Suppose $a \mid b$ and $b \mid c$. Then $b = ma$ and $c = nb$ for some $m, n \in \mathbb{Z}$. Thus $c = nma$, so $a \mid c$. $\square$

Problem 4. Let $a, b, c \in \mathbb{Z}$ be positive integers.
Show that $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$.

Solution. We have seen that

$$\gcd(a, b) = 1 \quad \Leftrightarrow \quad ax + by = 1 \text{ for some } x, y \in \mathbb{Z}.$$

($\Rightarrow$) Suppose that $\gcd(a, bc) = 1$. Then $ax + (bc)y = 1$ for some $x, y \in \mathbb{Z}$. Thus $ax + b(cy) = 1$, so $\gcd(a, b) = 1$. Also $ax + c(by) = 1$, so $\gcd(a, c) = 1$.

($\Leftarrow$) Suppose that $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$. Then $ax_1 + by_1 = 1$ and $ax_2 + cy_2 = 1$ for some $x_1, x_2, y_1, y_2 \in \mathbb{Z}$. Multiplying these equations gives

$$a(x_1 a x_2 + x_1 c y^2 + b y_1 x_2) + bc(y_1 y_2) = 1.$$

Thus $\gcd(a, bc) = 1$. $\square$

Problem 5. Find the additive order of $\overline{6}$, $\overline{11}$, $\overline{18}$, and $\overline{28}$ in $\mathbb{Z}_{36}$.

Solution. We have seen that the additive order of $\overline{a}$ in $\mathbb{Z}_n$ is $\operatorname{ord}_+(\overline{a}) = \frac{n}{\gcd(a,n)}$. Thus

$$\begin{aligned}
\operatorname{ord}_+(\overline{6}) &= \frac{36}{6} = 6 \\
\operatorname{ord}_+(\overline{11}) &= \frac{36}{1} = 36 \\
\operatorname{ord}_+(\overline{18}) &= \frac{36}{18} = 2 \\
\operatorname{ord}_+(\overline{28}) &= \frac{36}{4} = 9
\end{aligned}$$

$\square$

Problem 6. Find the multiplicative order of $\overline{10}$ in $\mathbb{Z}_{21}^*$.

Solution. Compute

$$\begin{aligned}
&\overline{10}^2 = \overline{100} = \overline{5} \\
&\overline{10}^3 = \overline{5} \cdot \overline{10} = \overline{50} = \overline{13} \\
&\overline{10}^4 = \overline{13} \cdot \overline{10} = \overline{-8} \cdot \overline{10} = \overline{-80} = \overline{-4} = \overline{4} \\
&\overline{10}^5 = \overline{4} \cdot \overline{10} = \overline{40} = \overline{-2} = \overline{19} \\
&\overline{10}^6 = \overline{19} \cdot \overline{10} = \overline{-2} \cdot \overline{10} = \overline{-20} = \overline{-1} = \overline{1}
\end{aligned}$$

Hence, $\operatorname{ord}_*(\overline{10}) = 6$. $\square$

Problem 7. Solve the equation $\overline{17}x = \overline{23}$ in $\mathbb{Z}_{71}$.

Solution. First, we use the Euclidean algorithm to find the inverse of $\overline{17}$ in $\mathbb{Z}_{71}$. This computation shows that

$$17(-25) + 71(6) = 1;$$

modding out by 71 yields $\overline{17} \cdot \overline{-25} = \overline{1}$, so $\overline{17}^{-1} = \overline{-25} = \overline{46}$. Multiplying both sides of $\overline{17}x = \overline{23}$ by $\overline{44}$ yields

$$x = \overline{4423} = \overline{46}.$$

$\square$

Problem 8. Solve the equation $x^2 - \overline{5}x - \overline{2} = \overline{0}$ in $\mathbb{Z}_{11}$.

Solution. In $\mathbb{Z}_{11}$, we have $\overline{-5} = \overline{6}$ and $\overline{-2} = \overline{9}$. So this equation becomes $x^2 + \overline{6}x + \overline{9} = (x + \overline{3})^2 = 0$. Since 11 is prime, $\mathbb{Z}_{11}$ has no zero divisors, so $x = -\overline{3} - \overline{8}$ is the only solution. $\square$