MTH 505: Number Theory — Spring 2017
Midterm Exam — Drew Armstrong

There are 10 parts and 5 pages. Each part is worth 3 points for a total of 30 points. No electronic devices are allowed. Anyone caught cheating will receive a score of zero.

Problem 1. (Division With Remainder) Assume that there exist integers $q, q', r, r' \in \mathbb{Z}$ with the properties

$$\begin{cases} 5 = 3q + r \\ 0 \leqslant r < 3 \end{cases} \quad \text{and} \quad \begin{cases} 5 = 3q' + r' \\ 0 \leqslant r' < 3. \end{cases}$$

In parts (a) and (b) you will prove that $r = r'$. So assume for contradiction that $(r - r') > 0$.

(a) Show that $3|(r-r')$ and then use the assumption $(r-r') > 0$ to prove that $3 \leqslant (r-r')$.

Proof. To see that $3|(r - r')$ note that

$$\begin{aligned} 3q + r &= 3q' + r' \\ r - r' &= 3q' - 3q = 3(q' - q). \end{aligned}$$

If $(r - r') > 0$ then from the above equation we must also have $(q' - q) > 0$. Since $q' - q$ is an integer this implies that

$$\begin{aligned} 1 &\leqslant (q' - q) \\ 3 &\leqslant 3(q' - q) = (r - r'). \end{aligned}$$

□

(b) Show that the inequalities $(0 \leqslant r < 3)$, $(0 \leqslant r' < 3)$ and $3 \leqslant (r - r')$ imply a contradiction. This completes the proof that $r = r'$.

Proof. The inequality $0 \leqslant r'$ implies that $r - r' \leqslant r$. But then the inequalities $r < 3$ and $3 \leqslant (r - r')$ give a contradiction:

$$3 \leqslant (r - r') \leqslant r < 3.$$

□

(c) Use the result of parts (a) and (b) to prove that there does **not exist** an integer $x \in \mathbb{Z}$ with the property $3x = 5$.

Proof. Assume for contradiction that there exists such an integer $x \in \mathbb{Z}$. Then we have

$$\begin{cases} 5 = 3x + 0 \\ 0 \leqslant 0 < 3 \end{cases} \quad \text{and} \quad \begin{cases} 5 = 3 \cdot 1 + 2 \\ 0 \leqslant 2 < 3. \end{cases}$$

By parts (a) and (b) these conditions imply that $0 = 2$, which is a contradiction. □

Problem 2. (Linear Diophantine Equations)

(a) Use the Vector Euclidean Algorithm to find **specific** integers $x', y' \in \mathbb{Z}$ such that

$$33x' + 14y' = 1.$$

Solution. We consider the set of triples $(x, y, z) \in \mathbb{Z}^3$ such that $33x+14y = z$. We apply the Euclidean Algorithm starting with the two obvious triples $(1, 0, 33)$ and $(0, 1, 14)$ to obtain:

x	y	z
1	0	33
0	1	14
1	−2	5
−2	5	4
3	−7	1
−14	33	0

The second-to-last row gives us the specific solution $33(3)+14(-7) = 1$. [In particular, this tells us that 33 and 14 are coprime.]

(b) Find **all** integers $x, y \in \mathbb{Z}$ such that

$$33x + 14y = 0.$$

Solution. The equation $33x = -14y$ and Euclid's Lemma tells us that y is a multiple of 33 and x is a multiple of 14, say $x = 14k$ and $y = 33\ell$ for $k, \ell \in \mathbb{Z}$. Then by substitution we have

$$\begin{aligned} 33(14k) &= -14(33\ell) \\ 462k &= -462\ell \end{aligned}$$

and canceling 462 from both sides gives $\ell = -k$. We conclude that the complete solution to $33x + 14y = 0$ is given by

$$(x, y) = (14k, -33k) \quad \text{for all } k \in \mathbb{Z}.$$

(c) Combine your answers from parts (a) and (b) to find **all** integers $x, y \in \mathbb{Z}$ such that

$$33x + 14y = 2.$$

Solution. From part (a) we have $33(3) + 14(-7) = 1$ and multiplying this by 2 gives the specific solution $33(6) + 14(-14) = 2$. Then we add this to the complete solution of the homogeneous equation from part (b) to obtain the complete solution

$$\begin{aligned} (x, y) &= (6, -14) + (14k, -33k) \\ &= (6 + 14k, -14 - 33k) \quad \text{for all } k \in \mathbb{Z}. \end{aligned}$$

There are infinitely many different ways to express this solution.

//

Problem 3. (Modular Arithmetic)

(a) Compute the multiplicative inverse of the element $[14]_{33}$ in the ring $\mathbb{Z}/33\mathbb{Z}$.

Solution. From Problem 2 we have $33(3) + 14(-7) = 1$ and reducing this equation mod 33 gives

$$\begin{aligned} [1]_{33} &= [14(-7)]_{33} + [33(3)]_33 3 \\ &= [14]_{33} \cdot [-7]_{33} + [33]_{33} \cdot [3]_{33} \\ &= [14]_{33} \cdot [-7]_{33} + [0]_{33} \cdot [3]_{33} \\ &= [14]_{33} \cdot [-7]_{33}. \end{aligned}$$

Hence the inverse is

$$[14^{-1}]_{33} = [-7]_{33} = [26]_{33}.$$

(b) Use your answer from part (a) to find **all** integers $x \in \mathbb{Z}$ such that $[14x]_{33} = [2]_{33}$.

Solution. We multiply both sides of the equation $[14]_{33} \cdot [x]_{33} = [2]_{33}$ by the inverse of $[14]_{33}$ to obtain

$$\begin{aligned} [14]_{33} \cdot [x]_{33} &= [2]_{33} \\ ([26]_{33} \cdot [14]_{33}) \cdot [x]_{33} &= [26]_{33} \cdot [2]_{33} \\ [1]_{33} \cdot [x]_{33} &= [26]_{33} \cdot [2]_{33} \\ [x]_{33} &= [52]_{33} \\ &= [19]_{33}. \end{aligned}$$

Hence the complete solution is $x = 19 + 33k$ for all $k \in \mathbb{Z}$.

(c) Compute the value of Euler's totient function $\varphi(33)$.

Solution. The prime factorization of 33 is $33 = 3 \cdot 11$, so we have

$$\varphi(33) = \varphi(3) \cdot \varphi(11) = (3 - 1)(11 - 1) = 2 \cdot 10 = 20.$$

(d) Use Euler's Totient Theorem to compute the remainder of 14^{19} mod 33. [Hint: Use parts (a) and (c) to compute the standard form the element $[14^{19}]_{33} \in \mathbb{Z}/33\mathbb{Z}$.]

Solution. Since $\gcd(14, 33) = 1$, Euler's Totient Theorem tells us that $[14^{20}]_{33} = [14^{\varphi(33)}] = [1]_{33}$. Then we can multiply both sides of this equation by $[14^{-1}]_{33} = [26]_{33}$ to obtain

$$\begin{aligned} [14^{20}]_{33} &= [1]_{33} \\ [14^{-1}]_{33} \cdot [14^{20}]_{33} &= [14^{-1}]_{33} \cdot [1]_{33} \\ [14^{19}]_{33} &= [14^{-1}]_{33} \\ &= [26]_{33}. \end{aligned}$$

We conclude that 14^{19} has remainder 26 modulo 33. //