MATH 405: Exam 1

Micah Sherry

February 22, 2025

1. Compute

   (a) 5^{36} in $\mathbb{Z}_{11}$
   $$5^{36} \equiv (5^2)^{18} \equiv (3)^{18} \equiv 9(9)^8 \equiv 9(4)^4 \equiv 9(5)^2 \equiv 9(3) \equiv 5 \pmod{11}$$

   (b) 5^{-3} in $\mathbb{Z}_{11}$
   since the $gcd(5, 11) = 1$, 5^{-1} exist in $\mathbb{Z}_{11}$. Notice, $11 - 2 * 5 = 1$. Therefore $5^{-1} \equiv -2 \pmod{11}$
   $$5^{-3} \equiv (-2)^3 \equiv -8 \equiv 3 \pmod{11}$$

2. Given the integers a, b below find gcd(a, b) using the Euclidean Algorithm and also find integers x, y such that $gcd(a, b) = ax + by$

   (a) $a = 3185$ and $b = 2873$
   $$\begin{aligned} 3185 &= 1(2873) &&+ 312 \\ 2873 &= 9(312) &&+ 65 \\ 312 &= 4(65) &&+ 52 \\ 65 &= 1(52) &&+ 13 \\ 52 &= 4(13) &&+ 0 \end{aligned}$$
   Therefore $gcd(a, b) = 13$.
   $$\begin{aligned} 13 &= (65) &&- (52) \\ 13 &= (65) &&- (312 - 4(65)) \\ 13 &= -(312) &&+ 5(65) \\ 13 &= -(312) &&+ 5(2873 - 9(312)) \\ 13 &= 5(2873) &&- 46(312) \\ 13 &= 5(2873) &&- 46(3185 - 2873) \\ 13 &= -46(3185) &&+ 51(2873) \end{aligned}$$
   Therefore $x = -46$ and $y = 51$ is a solution to $gcd(a, b) = ax + by$

   (b) $a = 360$ and $b = 343$
   $$\begin{aligned} 360 &= 1(343) &&+ 17 \\ 343 &= 20(17) &&+ 3 \\ 17 &= 5(3) &&+ 2 \\ 3 &= 1(2) &&+ 1 \end{aligned}$$
   Therefore $gcd(a, b) = 1$.

$$
\begin{aligned}
1 &= (3) && - (2) \\
1 &= (3) && - (17 - 5(3)) \\
1 &= -(17) && + 6(3) \\
1 &= -(17) && + 6(343 - 20(17)) \\
1 &= 6(343) && - 121(17) \\
1 &= 6(343) && - 121(360 - 343) \\
1 &= -121(360) && + 127(343)
\end{aligned}
$$

Therefore $x = -121$ and $y = 127$ is a solution to $gcd(a, b) = ax + by$

3. Let n be any integer. Prove that one of the three integers n, $n + 2$, or $n + 4$ must be a multiple of 3.

Proof. assume n is an integer. Notice there are three cases for n.

Case 1: $n \equiv 0 \pmod 3$. In this case n is a multiple of 3.

Case 2: $n \equiv 1 \pmod 3$. In this case $n + 2$ is a multiple of 3.

Case 3: $n \equiv 2 \pmod 3$. In this case $n + 4$ is a multiple of 3.

Therefore the statement is true. $\square$

4. Define a relationship $\lhd$ for points in $\mathbb{R}^2$ as follows.For $(x, y), (x_1, y_1) \in \mathbb{R}^2$, $(x, y) \lhd (x1, y1)$ if and only if $|x| = |x_1|$ and $|y| = |y_1|$.

   (a) Prove or disprove that the relationship $\lhd$ is reflexive

   Proof. Let $(x, y) \in \mathbb{R}^2$. Since $x = x$ and $y = y$, the relation $\lhd$ is reflexive $\square$

   (b) Prove or disprove that the relationship $\lhd$ is symmetric

   Proof. let $(x_0, y_0), (x_1, y_1) \in \mathbb{R}^2$ with $(x_0, y_0) \lhd (x_1, y_1)$.
   So, $|x_0| = |x_1|$ and $|y_0| = |y_1|$. Since equality is symmetric $|x_1| = |x_0|$ and $|y_1| = |y_0|$. Therefore $(x_1, y_1) \lhd (x_0, y_0)$, So $\lhd$ is symmetric.

   $\square$

   (c) Prove or disprove that the relationship $\lhd$ transitive

   Proof. Let $(x_0, y_0), (x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$, with $(x_0, y_0) \lhd (x_1, y_1)$ and $(x_1, y_1) \lhd (x_2, y_2)$.
   $(x_0, y_0) \lhd (x_1, y_1)$, implies $|x_0| = |x_1|$ and $|y_0| = |y_1|$.
   Similarly, $(x_1, y_1) \lhd (x_2, y_2)$, implies $|x_1| = |x_2|$ and $|y_1| = |y_2|$.
   Therefore, $|x_0| = |x_2|$ and $|y_0| = |y_2|$ and $(x_0, y_0) \lhd (x_2, y_2)$. Thus, the relation $\lhd$ is transitive. $\square$

5. Let a, b, k be integers. If $a|k$ and $b|k$ and $gcd(a, b) = 1$, then show $ab|k$.

Proof. Assume $a|k$ and $b|k$ and $gcd(a, b) = 1$. Since, $a|k$ then $k = ak_0$, for some $k_0 \in \mathbb{Z}$. Similarly, $b|k$ implies $k = bk_1$, for some $k_1 \in \mathbb{Z}$.
Since $gcd(a, b) = 1$ then there exist x and y such that $ax + by = 1$ So,

$$
\begin{aligned}
akx + bky &= k \\
abk_1x + bak_0y &= k \\
ab(k_1x + k_0y) &= k
\end{aligned}
$$

Therefore $ab|k$. $\square$

6. Let p be a prime. Show that in $\mathbb{Z}_p$ the only solutions to $x_2 \equiv_p 1$ are 1 and $p-1$.

Proof. Consider, the following concurrences

$$\begin{aligned} x^2 &\equiv_p 1 \\ x^2 - 1 &\equiv_p 0 && \text{(subtracting 1 from both sides)} \\ (x-1)(x+1) &\equiv_p 0 && \text{(factoring)} \end{aligned}$$

Since p is prime $x-1$ or $x+1$ must be congruent to 0. This implies that $x \equiv_p 1$ or $x \equiv_p -1 \equiv_p p-1$.

□