Problem Set 2 - Thomas Boyko - 30191728

1. (a) Solve $5x \equiv 11 \pmod{37}$ and $11y \equiv 5 \pmod{37}$.

   First we will solve for x. Note that this equation has a solution since $GCD(5, 37) = 1$. Transform the equivalence into a Diophantine equation. We have $5x + 37a = 11$. We now can use the Euclidean algorithm to find x, a.

   This gives the equation $1 = -2(37) + 15(5)$, which we can multiply by 11 to obtain $11 = -22(37) + 165(5)$.

   We can take this $\pmod{37}$ to give us $11 \equiv 165(5) \equiv 17(5) \pmod{37}$.

   So $x \equiv 17 \pmod{37}$.

   Now we can find y. Note that this equation is solvable since $GCD(11, 37) = 1$ and it provides the Diophantine equation $11y + 37b = 5$.

   Solving this equation gives the solution $1 = 3(37) - 10(11)$, which can be multiplied by 5 to give us $5 = 15(37) - 50(11)$. Reducing this $\pmod{3}7$ again gives $5 \equiv -50(11) \equiv 24(11) \pmod{37}$, which shows that $x \equiv 24 \pmod{37}$.

   (b) Suppose your solutions are x_0 and y_0. What is the relationship between $[x_0]$ and $[y_0]$ in $\mathbb{Z}_{37}$?

   We can see computationally that $[x_0][y_0] = [x_0 y_0] = [408] = [1]$. So x_0 and y_0 are multiplicative inverses for each other in $\mathbb{Z}_{37}$.

2. Use repeated squaring method to simplify $12^{149} \pmod{15}$.

   First we will calcluate repeated squares, until we obtain $12^{128} \pmod{15}$.

$$
\begin{aligned}
12 &\equiv 12 \pmod{15} \\
12^2 &\equiv 144 \equiv 9 \pmod{15} \\
12^4 &\equiv 81 \equiv 6 \pmod{15} \\
12^8 &\equiv 36 \equiv 6 \pmod{15} \\
12^{16} &\equiv 36 \equiv 6 \pmod{15} \\
12^{32} &\equiv 36 \equiv 6 \pmod{15} \\
12^{64} &\equiv 36 \equiv 6 \pmod{15} \\
12^{128} &\equiv 36 \equiv 6 \pmod{15}
\end{aligned}
$$

.

   We can see from above that 6^n for any positive n is equivalent to $6 \pmod{15}$.

   Now we must find the binary representation for 149. We find that $149 = 128 + 16 + 4 + 1$.

   So we may write $12^{149} \equiv 12^{128}12^{16}12^{4}12^{1} \equiv (6)(6)(6)(12) \equiv (6)(12) \equiv 72 \equiv 12 \pmod{15}$.

   So $12^{149} \equiv 12 \pmod{15}$.

3. Let p be a prime number.

   (a) Show that $\binom{p}{k} \equiv 0 \pmod{p}$ for all $k \in \mathbb{Z}$ with $1 \leq k < p$.

   Proof. Consider:

$$
\begin{aligned}
\binom{p}{k} &= \frac{p!}{k!(p-k)!} = \frac{p(p-1)!}{k!(p-k)!} \\
\binom{p}{k} k!(p-k)! &= p(p-1)!
\end{aligned}
$$

.

   Since $\binom{p}{k}$ is an integer, $k!(p-k)! | p(p-1)!$. So $k!(p-k)!$ must divide $(p-1)!$ since p is prime. This means $\frac{(p-1)!}{k!(p-k)!} \in \mathbb{Z}$, and $p | \binom{p}{k}$ which means $\binom{p}{k} \equiv 0 \pmod{p}$. □

   (b) Show that for all integers x, y, $(x + y)^p \equiv x^p + y^p \pmod{p}$.

Proof. We begin by writing $(x+y)^p$ according to the binomial expansion.

$$\begin{aligned}(x+y)^p &= \sum_{k=0}^{p} \binom{p}{k} x^{p-k} y^k \\ &= x^p + y^p + \sum_{k=1}^{p-1} \binom{p}{k} x^{p-k} y^k\end{aligned}$$

$\pmod p$, this gives us:

$$(x+y)^p \equiv x^p + y^p + \sum_{k=1}^{p-1} \binom{p}{k} x^{p-k} y^k \pmod p.$$

And since we know that $\binom{p}{k} \equiv 0$ for $1 \le k \le p-1$, we can say that

$$(x+y)^p \equiv x^p + y^p \pmod p.$$

$\square$

4. Deduce from the previous problem : for all integers $a, a^p \equiv a \pmod p$.

   Proof. Argue by induction. Let p be prime and suppose $(a+b)^p \equiv a^p + b^p \pmod p$.
   Base case: $a \equiv 0 \pmod p$: $a^p w \equiv 0^p \equiv 0 \equiv a \pmod p$.
   So the base case holds.
   Inductive Hypothesis: Let $k \in \mathbb{Z}_p$ and suppose $k^p \equiv k \pmod p$. We must show that $(k+1)^p \equiv k+1 \pmod p$.
   $(k+1)^p \equiv k^p + 1^p \equiv k+1 \pmod p$.
   So for a prime p and any integer a, $a^p \equiv a \pmod p$. $\square$

5. Show that the polynomial $x^6 + 45x^4 - 10x^2 + 5x - 2$ has no integer solution.

   Proof. Consider $f(x) \pmod 5$

   $$x^6 + 45x^4 - 10x^2 + 5x - 2 \equiv x^6 - 2 \pmod 5.$$

   So we have
   $$x^6 \equiv 2 \pmod 5.$$

   We can check by cases:

   $$\begin{aligned}0^6 &\equiv 0 \pmod 5\\ 1^6 &\equiv 1 \pmod 5\\ 2^6 &\equiv 4 \pmod 5\\ 3^6 &\equiv 4 \pmod 5\\ 4^6 &\equiv 1 \pmod 5.\end{aligned}$$

   And since $\exists m \in \mathbb{Z}$ so that $f(x) \pmod m$ has no integer solutions, f has no integer solutions. $\square$