Math 110A Homework 2

Jiaping Zeng

1/17/2021

1. (a) Which of $[0], [1], [2], [3]$ is equal to $[5^{2000}]$ in $\mathbb{Z}/4\mathbb{Z}$?

   Answer: Since $5 \equiv 1 \pmod 4$, by repeatedly applying Theorem 2.2 we have $5^{2000} \equiv 1^{2000} = 1 \pmod 4$. Then by Theorem 2.3 $[5^{2000}] \equiv [1] \pmod 4$.

   (b) Which of $[0], [1], [2], [3], [4]$ is equal to $[4^{2001}]$ in $\mathbb{Z}/5\mathbb{Z}$?

   Answer: Since $4 \equiv -1 \pmod 5$, by repeatedly applying Theorem 2.2 we have $4^{2001} \equiv (-1)^{2001} = -1 \pmod 5$. Then by Theorem 2.3 $[4^{2001}] \equiv [-1] \equiv [4] \pmod 5$.

2. If $a \in \mathbb{Z}$, prove that a^2 is not congruent to 2 or 3 modulo 4.

   Answer: By Corollary 2.5, a must be congruent to one of $0, 1, 2, 3 \pmod 4$. Then by Theorem 2.2, a^2 must be congruent to one of $0^2, 1^2, 2^2, 3^2$. Note that $2^2 = 4 \equiv 0 \pmod 4$ and $3^2 = 9 \equiv 1 \pmod 4$, therefore a^2 can only be congruent to 0 or 1.

3. (a) Prove or disprove: If $a^2 \equiv b^2 \pmod n$, then $a \equiv b \pmod n$ or $a \equiv -b \pmod n$.

   Answer: Disprove by counter example: let $a = 2$ and $b = 4$, then $a^2 = 4 \equiv 16 = b^2 \pmod 4$. However, $2 \not\equiv 4 \pmod 4$ and $2 \not\equiv -4 \pmod 4$.

   (b) Do part (a) when n is prime.

   Answer: By definition, $a^2 \equiv b^2$ (mod n) implies that n divides $a^2 - b^2$. By difference of squares, n divides $(a+b)(a-b)$, then since n is prime it must divide either $a+b$ or $a-b$ by Theorem 1.5. If n divides $a+b$, $a \equiv -b \pmod n$ by definition and if n divides $a-b$, $a \equiv b \pmod n$.

4. *Fermat's Little Theorem.* Let p be a positive prime number.

   (a) Prove that for any $a, b \in \mathbb{Z}$, $(a+b)^p \equiv a^p + b^p \pmod p$.

   Answer: By binomial theorem, $(a+b)^p = \sum_{m=0}^{p} \binom{p}{m} a^m b^{p-m}$. By exercise 1.3.25, p divides $\binom{p}{k}$ for $1 \leq k \leq p-1$, i.e. p divides every term in the polynomial except the two with coefficients $\binom{p}{0}$ and $\binom{p}{p}$, which corresponds to the terms $\binom{p}{0} b^p = b^p$ and $\binom{p}{p} a^p = a^p$. Since the other terms are divisible by p, by Theorem 2.3 they are congruent to $0 \pmod p$. Therefore $(a+b)^p \equiv a^p + b^p$.

   (b) Prove by induction that $a^p \equiv a \pmod p$ for all nonnegative integers a.

   Answer: By induction on a.

   Base case: $a = 1$, then clearly $1^p = 1$ is true for any p.

   Induction step: suppose $a^p \equiv a \pmod p$, we want to show that $(a+1)^p \equiv a+1 \pmod p$. This is trivial upon substituting $b = 1$ into part (a).

   Therefore $a^p \equiv a \pmod p$ for $a \geq 1$.

(c) Prove that if $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Answer: Since $p \nmid a \implies (a, p) = 1$, by Theorem 2.10 a is a unit in $\mathbb{Z}/p\mathbb{Z}$ with an inverse b such that $ab = 1$. By part (b), $a \equiv a^p \pmod{p}$, so $ab = 1 \implies a^p b \equiv 1 \implies a^{p-1}(ab) \equiv 1 \implies a^{p-1} \equiv 1 \pmod{p}$.

(d) Find the remainder when 3^{1000} is divided by 7, without using a calculator or computer.

Answer: Since $7 \nmid 3$, we know that $3^6 \equiv 1 \pmod{7}$ by part (c). Then $3^{1000} = 3^{6^{166}} \cdot 3^4 \equiv 3^4 = 81 \equiv 4 \pmod{7}$. Therefore the remainder is 4.

5. Write out the addition and multiplication tables for

(a) $\mathbb{Z}/4\mathbb{Z}$

Answer:

$\oplus$	[0]	[1]	[2]	[3]
[0]	0	1	2	3
[1]	1	2	3	0
[2]	2	3	0	1
[3]	3	0	1	2

$\odot$	[0]	[1]	[2]	[3]
[0]	0	0	0	0
[1]	0	1	2	3
[2]	0	2	0	2
[3]	0	3	2	1

(b) $\mathbb{Z}/7\mathbb{Z}$

Answer:

$\oplus$	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	0	1	2	3	4	5	6
[1]	1	2	3	4	5	6	0
[2]	2	3	4	5	6	0	1
[3]	3	4	5	6	0	1	2
[4]	4	5	6	0	1	2	3
[5]	5	6	0	1	2	3	4
[6]	6	0	1	2	3	4	5

$\odot$	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	0	0	0	0	0	0	0
[1]	0	1	2	3	4	5	6
[2]	0	2	4	6	1	3	5
[3]	0	3	6	2	5	1	4
[4]	0	4	1	5	2	6	3
[5]	0	5	3	1	6	4	2
[6]	0	6	5	4	3	2	1

6. Solve the equation $x^2 \oplus [3] \odot x \oplus [2] = [0]$ in $\mathbb{Z}/6\mathbb{Z}$.

Answer:

x	$x^2 \oplus [3] \odot x \oplus [2]$	is solution?
[0]	$[0] \odot [0] \oplus 3 \odot [0] \oplus 2 = [0] + [0] + [2] = [2]$	yes
[1]	$[1] \odot [1] \oplus 3 \odot [1] \oplus 2 = [1] + [3] + [2] = [0]$	no
[2]	$[2] \odot [2] \oplus 3 \odot [2] \oplus 2 = [4] + [0] + [2] = [0]$	no
[3]	$[3] \odot [3] \oplus 3 \odot [3] \oplus 2 = [3] + [3] + [2] = [2]$	yes
[4]	$[4] \odot [4] \oplus 3 \odot [4] \oplus 2 = [2] + [0] + [2] = [4]$	no
[5]	$[5] \odot [5] \oplus 3 \odot [5] \oplus 2 = [1] + [3] + [2] = [0]$	no

Therefore the equation has two solutions: [0] and [2].

7. (a) Find an element $[a]$ in $\mathbb{Z}/7\mathbb{Z}$ such that every nonzero element of $\mathbb{Z}/7\mathbb{Z}$ is a power of $[a]$.

Answer: Let $a = 3$, then we have $[a] = [3], [a]^2 = [2], [a]^3 = [6], [a]^4 = [4], [a]^5 = [5], [a]^6 = [1]$ as desired.

(b) Do (a) in $\mathbb{Z}/5\mathbb{Z}$.

Answer: Again let $a = 3$, then we have $[a] = [3], [a]^2 = [4], [a]^3 = [2], [a]^4 = [1]$ as desired.

(c) Can you do (a) in $\mathbb{Z}/6\mathbb{Z}$?

Answer: No. If we pick an odd a then a^n would also be odd and $[a]^n$ would not contain the even classes (since $a^n - 6k$ would be odd for any k); similarly if we pick an even a then all powers would be even and $[a]^n$ would not contain the odd classes.

8. Find all units and zero divisors in

(a) $\mathbb{Z}/8\mathbb{Z}$

Answer: $1, 3, 5, 7$ are units in $\mathbb{Z}/8\mathbb{Z}$ because $3 \cdot 3 = 1$, $5 \cdot 5 = 1$ and $7 \cdot 7 = 1$; $2, 4$ are zero divisors because $2 \cdot 4 = 0$.

(b) $\mathbb{Z}/9\mathbb{Z}$

Answer: $1, 2, 4, 5, 7, 8$ are units in $\mathbb{Z}/9\mathbb{Z}$ because $2 \cdot 5 = 1$, $4 \cdot 7 = 1$ and $8 \cdot 8 = 1$; 3 is a zero divisor because $3 \cdot 3 = 0$.

(c) $\mathbb{Z}/10\mathbb{Z}$

Answer: $1, 3, 7, 9$ are units in $\mathbb{Z}/10\mathbb{Z}$ because $3 \cdot 7 = 1$ and $9 \cdot 9 = 1$; $2, 5$ are zero divisors because $2 \cdot 5 = 0$.

9. Let a, b, n be integers with $n > 1$. Let $d = (a, n)$ and assume that $d|b$. Prove that the equation $[a]x = [b]$ has exactly d solutions in $\mathbb{Z}/n\mathbb{Z}$ as follows:

(a) Explain why there are integers u, v, a_1, b_1, n_1 such that $au+nv = d$, $a = da_1$, $b = db_1$ and $n = dn_1$.

Answer: By Theorem 1.2, since $d = (a, n)$ there must exist $u, v \in \mathbb{Z}$ such that $au + nv = d$. By definition of gcd, $d = (a, n)$ divides both a and n; in addition, it is given that d divides b. Then by definition of divisibility there exists $a_1, b_1, n_1 \in \mathbb{Z}$ such that $a = da_1$, $b = db_1$ and $n = dn_1$.

(b) Show that each of $[ub_1], [ub_1 + n_1], [ub_1 + 2n_1], \ldots, [ub_1 + (d-1)n_1]$ is a solution of $[a]x = [b]$.

Answer: Define k such that $0 \leq k \leq d - 1$, then we want to show that each of $[ub_1 + kn_1]$ is a solution. By substitution we have $[a][ub_1 + kn_1] = [aub_1 + akn_1] = [(d - nv)b_1 + da_1kn_1] = [db_1 - nvb_1 + dn_1a_1k = [b - n(vb_1 + a_1k)]$. Note that $[b - n(vb_1 + a_1k)] \equiv [b] \pmod{n}$, so each of $[ub_1 + kn_1]$ is a solution of $[a]x = [b]$.

(c) Show that the solutions listed in part (b) are all distinct.

Answer: Take distinct and arbitrary k_1, k_2 such that $0 \leq k_1, k_2 \leq d - 1$, we want to show that $[ub_1 + k_1n_1] \neq [ub_1 + k_2n_1]$. By taking the difference we have $[ub_1 + k_1n_1] - [ub_1 + k_2n_1] = [(k_1 - k_2)n_1]$. However $n = dn_1 \nmid (k_1 - k_2)n_1$ as we would need $(k_1 - k_2)$ to be a multiple of d, which is not possible by our constraint $0 \leq k_1, k_2 \leq d - 1$. Therefore the solutions listed in part (b) are distinct.

(d) If $x = [r]$ is any solution of $[a]x = [b]$, show that $[r] = [ub_1] + [kn_1]$ for some integer k with $0 \leq k \leq d - 1$.

Answer: Since $x = [r]$ is a solution as given, we have $[a][r] = [b] \implies [ar] - [b] = [0]$. As shown in part (b), $x = [ub_1]$ is also a solution, i.e. $[a][ub_1] = [b]$. By substitution we have $[ar] - [aub_1] = [0]$, therefore $[ar] \equiv [aub_1] \pmod{n}$ and $n|(ar - aub_1)$ by definition of congruence. Then since $n = dn_1$ and $a = da_1$, we have $dn_1|da_1(r - ub_1) \implies n_1|a_1(r - ub_1)$. Since a_1 and n_1 are constructed by factoring out the gcd of a and n, we know that $(a_1, n_1) = 1$. Therefore by Theorem 1.4 we have $n_1|(r - ub_1)$, i.e. there exist some $k \in \mathbb{Z}$ such that $kn_1 = r - ub_1 \implies r = ub_1 + kn_1 \implies [r] = [ub_1 + kn_1]$.

10. Use Problem 9 to solve the following equations:

    (a) $15x = 9$ in $\mathbb{Z}/18\mathbb{Z}$

    Answer: We have $a = 15, b = 9$ and $n = 18$, then $d = (a, n) = 3$, $b_1 = b/d = 3$ and $n_1 = n/d = 6$. We can then take $u = -1$ and $v = 1$ to have $au + nv = d$. Then by the problem 9(b), the solutions are $[-3], [-3 + 6], [-3 + 12]$ which are congruent to $[15], [3], [9]$ respectively.

    (b) $25x = 10$ in $\mathbb{Z}/65\mathbb{Z}$.

    Answer: We have $a = 25, b = 10$ and $n = 65$, then $d = (a, n) = 5$, $b_1 = b/d = 2$ and $n_1 = n/d = 13$. We can then take $u = -5$ and $v = 2$ to have $au + nv = d$. Then by the problem 9(b), the solutions are $[-10], [-10 + 13], [-10 + 26], [-10 + 39], [-10 + 52]$ which are congruent to $[55], [3], [16], [29], [42]$ respectively.