

## Homework 7

ALECK ZHAO

April 14, 2017

15.1 For each of the following congruences, find all integers  $N$ , with  $N > 1$ , that make the congruence true.

(a)  $23 \equiv 13 \pmod{N}$

*Solution.* We have  $N \mid (23 - 13) \implies N \mid 10$ . Thus the possibilities are  $N \in \{2, 5, 10\}$ .  $\square$

(b)  $10 \equiv 5 \pmod{N}$

*Solution.* We have  $N \mid (10 - 5) \implies N \mid 5$ . Thus the only possibility is  $N = 5$ .  $\square$

(c)  $6 \equiv 60 \pmod{N}$

*Solution.* We have  $N \mid (6 - 60) \implies N \mid -54$ . Thus the possibilities are  $N \in \{2, 3, 6, 9, 18, 27, 54\}$ .  $\square$

(d)  $23 \equiv 22 \pmod{N}$

*Solution.* We have  $N \mid (23 - 22) \implies N \mid 1$ . For  $N > 1$ , this is impossible.  $\square$

2. Let  $a, b, c, n \in \mathbb{Z}$  with  $n > 1$ . Suppose  $a \equiv b \pmod{n}$ . Prove

(a)  $a + c \equiv b + c \pmod{n}$

*Proof.*

$$a \equiv b \pmod{n} \iff n \mid (a - b) \iff n \mid [(a + c) - (b + c)] \iff a + c \equiv b + c \pmod{n}$$
 $\square$

(b)  $ac \equiv bc \pmod{n}$

*Proof.*

$$a \equiv b \pmod{n} \iff n \mid (a - b) \implies n \mid c(a - b) \iff n \mid (ac - bc) \iff ac \equiv bc \pmod{n}$$
 $\square$

3. Let  $a, b$  be positive integers. Use the Division Algorithm Theorem to prove

$$(a + b) \pmod{n} = [(a \pmod{n}) + (b \pmod{n})] \pmod{n}$$

*Proof.* By the Division Algorithm Theorem, we write  $a = nq_1 + r_1$  and  $b = nq_2 + r_2$  for  $q_1, q_2, r_1, r_2 \in \mathbb{N}$  with  $0 \leq r_1, r_2 < n$  and  $q_1, q_2, r_1, r_2$  are unique. Then  $a \pmod{n} = r_1$  and  $b \pmod{n} = r_2$ .

Now, we have

$$a + b = (nq_1 + r_1) + (nq_2 + r_2) = n(q_1 + q_2) + (r_1 + r_2)$$

Then we may apply the Division Algorithm Theorem to  $r_1 + r_2 = (a \pmod{n}) + (b \pmod{n})$ :

$$r_1 + r_2 = nq_3 + r_3$$

for  $q_3, r_3 \in \mathbb{N}$  and  $0 \leq r_3 < n$  so  $r_3 = [(a \bmod n) + (b \bmod n)] \bmod n$ . Substituting, we have

$$a + b = n(q_1 + q_2) + (r_1 + r_2) = n(q_1 + q_2) + (nq_3 + r_3) = n(q_1 + q_2 + q_3) + r_3$$

However, applying the Division Algorithm Theorem directly to  $a + b$ , we have

$$a + b = nq + r \implies a + b \equiv r \pmod{n}$$

for  $q, r \in \mathbb{N}$  and  $0 \leq r < n$ . Since this is unique for  $a + b$ , it follows that  $r = r_3$ , as desired.  $\square$

4. Use Euclid's GCD Algorithm to find  $\gcd(a, b)$  for the numbers  $a$  and  $b$  listed below. Then, for each  $a$  and  $b$ , find integers  $x$  and  $y$  such that  $ax + by = \gcd(a, b)$ .

(a)  $a = 57, b = 21$

*Solution.*

$$57 \pmod{21} \equiv 15 \implies \gcd(57, 21) = \gcd(21, 15)$$

$$21 \pmod{15} \equiv 6 \implies \gcd(21, 15) = \gcd(15, 6)$$

$$15 \pmod{6} \equiv 3 \implies \gcd(15, 6) = \gcd(6, 3)$$

$$6 \pmod{3} \equiv 0 \implies \gcd(57, 21) = \boxed{3}$$

Now, we have

$$57 = 2 \cdot 21 + 15$$

$$21 = 1 \cdot 15 + 6$$

$$15 = 2 \cdot 6 + 3$$

so substituting backwards, we have

$$3 = 15 - 2 \cdot 6$$

$$= 15 - 2 \cdot (21 - 1 \cdot 15) = 3 \cdot 15 - 2 \cdot 21$$

$$= 3 \cdot (57 - 2 \cdot 21) - 2 \cdot 21 = 3 \cdot 57 - 8 \cdot 21$$

so  $(x, y) = (3, -8)$ .  $\square$

(b)  $a = 4321, b = 9876$

*Solution.* We may reverse the order of  $a$  and  $b$ , because  $\gcd(a, b) = \gcd(b, a)$ .

$$9876 \pmod{4321} \equiv 1234 \implies \gcd(9876, 4321) = \gcd(4321, 1234)$$

$$4321 \pmod{1234} \equiv 619 \implies \gcd(4321, 1234) = \gcd(1234, 619)$$

$$1234 \pmod{619} \equiv 615 \implies \gcd(1234, 619) = \gcd(619, 615)$$

$$619 \pmod{615} \equiv 4 \implies \gcd(619, 615) = \gcd(615, 4)$$

$$615 \pmod{4} \equiv 3 \implies \gcd(615, 4) = \gcd(4, 3)$$

$$4 \pmod{3} \equiv 1 \implies \gcd(4, 3) = \gcd(3, 1)$$

$$3 \pmod{1} \equiv 0 \implies \gcd(9876, 4321) = \boxed{1}$$

Now, we have

$$9876 = 2 \cdot 4321 + 1234$$

$$4321 = 3 \cdot 1234 + 619$$

$$1234 = 1 \cdot 619 + 615$$

$$619 = 1 \cdot 615 + 4$$

$$615 = 153 \cdot 4 + 3$$

$$4 = 1 \cdot 3 + 1$$

so substituting backwards, we have

$$\begin{aligned}
 1 &= 4 - 1 \cdot 3 \\
 &= 4 - 1 \cdot (615 - 153 \cdot 4) = 154 \cdot 4 - 1 \cdot 615 \\
 &= 154 \cdot (619 - 1 \cdot 615) - 1 \cdot 615 = 154 \cdot 619 - 155 \cdot 615 \\
 &= 154 \cdot 619 - 155 \cdot (1234 - 1 \cdot 619) = 309 \cdot 619 - 155 \cdot 1234 \\
 &= 309 \cdot (4321 - 3 \cdot 1234) - 155 \cdot 1234 = 309 \cdot 4321 - 1082 \cdot 1234 \\
 &= 309 \cdot 4321 - 1082 \cdot (9876 - 2 \cdot 4321) = 2473 \cdot 4321 - 1082 \cdot 9876
 \end{aligned}$$

so  $(x, y) = (-1082, 2473)$ . □

(c)  $a = 67890, b = 12345$

*Solution.*

$$\begin{aligned}
 67890 \pmod{12345} &\equiv 6165 \implies \gcd(67890, 12345) = \gcd(12345, 6165) \\
 12345 \pmod{6165} &\equiv 15 \implies \gcd(12345, 6165) = \gcd(6165, 15) \\
 6165 \pmod{15} &\equiv 0 \implies \gcd(67890, 12345) = \boxed{15}
 \end{aligned}$$

Now, we have

$$\begin{aligned}
 67890 &= 5 \cdot 12345 + 6165 \\
 12345 &= 2 \cdot 6165 + 15
 \end{aligned}$$

so substituting backwards, we have

$$\begin{aligned}
 15 &= 12345 - 2 \cdot 6165 \\
 &= 12345 - 2 \cdot (67890 - 5 \cdot 12345) = 11 \cdot 12345 - 2 \cdot 67890
 \end{aligned}$$

so  $(x, y) = (11, -2)$ . □

5. Let  $a$  and  $b$  be positive integers. Explain why  $\gcd(a, b) = \gcd(a, a + b)$ .

*Solution.* We have  $ax + by = a(x - y) + (a + b)y$ . If we minimize  $ax + by$  over the positive integers then we obtain  $\gcd(a, b)$ , but minimizing  $a(x - y) + (a + b)y$  gives  $\gcd(a, a + b)$ . Obviously these two minimums must be the same, so  $\gcd(a, b) = \gcd(a, a + b)$ . □

36.15 Suppose that  $a$  and  $b$  are relatively prime integers and that  $a \mid c$  and  $b \mid c$ . Prove that  $(ab) \mid c$ .

*Proof.* Let  $m, n \in \mathbb{Z}$  such that  $c = am = bn$ . Then since  $\gcd(a, b) = 1$ , there exist  $x, y \in \mathbb{Z}$  such that  $ax + by = 1$ . Then

$$\begin{aligned}
 c(ax + by) &= acx + bcy = a(bn)x + b(am)y = (ab)(nx + by) \\
 c(ax + by) &= c
 \end{aligned}$$

Thus,  $c = (ab)(nx + by)$  so  $(ab) \mid c$  as desired. □

7. Please find all solutions in  $\mathbb{Z}/n\mathbb{Z}$  for the following expressions.

37.2 (d)  $342 \otimes x \oplus 448 = 73$  in  $\mathbb{Z}/1003\mathbb{Z}$ .

*Solution.* We can subtract the constant term from both sides:

$$342 \otimes x \oplus 448 \equiv 73 \implies 342 \otimes x \equiv 73 \ominus 448 \equiv 628 \pmod{1003}$$

Now, we have

$$\begin{aligned} 1003 &= 2 \cdot 342 + 319 \\ 342 &= 1 \cdot 319 + 23 \\ 319 &= 13 \cdot 23 + 20 \\ 23 &= 1 \cdot 20 + 3 \\ 20 &= 6 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \end{aligned}$$

so substituting backwards, we have

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ &= 3 - 1 \cdot (20 - 6 \cdot 3) = 7 \cdot 3 - 1 \cdot 20 \\ &= 7 \cdot (23 - 1 \cdot 20) - 1 \cdot 20 = 7 \cdot 23 - 8 \cdot 20 \\ &= 7 \cdot 23 - 8 \cdot (319 - 13 \cdot 23) = 111 \cdot 23 - 8 \cdot 319 \\ &= 111 \cdot (342 - 1 \cdot 319) - 8 \cdot 319 = 111 \cdot 342 - 119 \cdot 319 \\ &= 111 \cdot 342 - 119 \cdot (1003 - 2 \cdot 342) = 349 \cdot 342 - 119 \cdot 1003 \end{aligned}$$

Thus  $349 \cdot 342 = 1 + 119 \cdot 1003 \equiv 1 \pmod{1003}$ , so  $342^{-1} = 349$ , and finally

$$x \equiv 628 \otimes 342^{-1} \equiv 628 \otimes 349 \equiv \boxed{518} \pmod{1003}$$

□

37.3 (c)  $9 \otimes x = 4$  in  $\mathbb{Z}/12\mathbb{Z}$ .

*Solution.* Since  $\gcd(12, 9) = 3 \neq 1$ , the inverse of 9 does not exist in  $\mathbb{Z}/12\mathbb{Z}$ , so there is no solution for  $x$ . □

37.4 (b)  $x \otimes x = 11$  in  $\mathbb{Z}/13\mathbb{Z}$ .

*Solution.* This is easy to check:

$$\begin{aligned} 1 \otimes 1 &\equiv 1 \\ 2 \otimes 2 &\equiv 4 \\ 3 \otimes 3 &\equiv 9 \\ 4 \otimes 4 &\equiv 3 \\ 5 \otimes 5 &\equiv 12 \\ 6 \otimes 6 &\equiv 10 \\ 7 \otimes 7 &\equiv 10 \\ 8 \otimes 8 &\equiv 12 \\ 9 \otimes 9 &\equiv 3 \\ 10 \otimes 10 &\equiv 9 \\ 11 \otimes 11 &\equiv 4 \\ 12 \otimes 12 &\equiv 1 \end{aligned}$$

Thus there are no solutions for  $x$  since the above are all possibilities, and none are 11. □

- 37.14 (a) In the context of  $\mathbb{Z}/n\mathbb{Z}$ , prove or disprove:  $a^b = a^{b \bmod n}$ .

*Proof.* This is not true. Let  $n = 5, a = 2, b = 7$ . Then

$$\begin{aligned} a^b &= 2^7 = 128 \equiv 3 \pmod{5} \\ a^{b \bmod n} &= 2^{7 \bmod 5} = 2^2 \equiv 4 \pmod{5} \end{aligned}$$

□

- (b) Find the value of  $3^{64}$  in  $\mathbb{Z}/100\mathbb{Z}$ .

*Solution.* We have

$$\begin{aligned} 3^2 &= 3 \cdot 3 \equiv 9 \pmod{100} \\ 3^4 &= 3^2 \cdot 3^2 \equiv 9 \cdot 9 \pmod{100} = 81 \pmod{100} \\ 3^8 &= 3^4 \cdot 3^4 \equiv 81 \cdot 81 \pmod{100} = 6561 \pmod{100} \equiv 61 \pmod{100} \\ 3^{16} &= 3^8 \cdot 3^8 \equiv 61 \cdot 61 \pmod{100} = 3721 \pmod{100} \equiv 21 \pmod{100} \\ 3^{32} &= 3^{16} \cdot 3^{16} \equiv 21 \cdot 21 \pmod{100} = 441 \pmod{100} \equiv 41 \pmod{100} \\ 3^{64} &= 3^{32} \cdot 3^{32} \equiv 41 \cdot 41 \pmod{100} = 1681 \pmod{100} \equiv 81 \pmod{100} \end{aligned}$$

□

- (c) Estimate how many multiplications you need to do to calculate  $a^b$  in  $\mathbb{Z}/n\mathbb{Z}$ .

**Answer.** Since we can replicate the above method, we would need roughly  $\log_2 b$  multiplications.

- (d) Give a sensible definition for  $a^0$  in  $\mathbb{Z}/n\mathbb{Z}$ .

**Answer.** We define  $a^0 := 1$ . This is the same as in  $\mathbb{Z}$ .

- (e) Give a sensible definition for  $a^b$  in  $\mathbb{Z}/n\mathbb{Z}$  when  $b < 0$ .

**Answer.** Since  $b < 0$ , there is already a definition for  $a^{-b}$ . Then since  $a^b \cdot a^{-b} = 1$ , we define  $a^b$  to be the multiplicative inverse of  $a^{-b}$ , if it exists.