

# MATH 332 - ALGEBRA AND NUMBER THEORY : HOMEWORK 4

## 1. CHAPTER 2: CONGRUENCES

**Exercises (pp. 65, 66):** 31, 32, 36, 38, 41.

**Proof of Exercise 31.** We need to find the 2 smallest positive integers  $x$  such that

$$\begin{cases} x \equiv 2 \pmod{7} \\ x \equiv 3 \pmod{11} \\ x \equiv 4 \pmod{13} \end{cases} \quad \begin{array}{l} \text{Obviously } 7, 11, 13 \text{ are pairwise coprime, so by the CRT this} \\ \text{system has a (unique) solution mod } 7 \times 11 \times 13 = 1001. \end{array}$$

As in the proof of the Chinese Remainder Theorem (2.11), we solve

$$\begin{cases} (11 \times 13)b_1 \equiv 1 \pmod{7} \iff 3b_1 \equiv 1 \pmod{7} \iff b_1 \equiv 5 \pmod{7} \\ (7 \times 13)b_2 \equiv 1 \pmod{11} \iff 3b_2 \equiv 1 \pmod{11} \iff b_2 \equiv 4 \pmod{11} \\ (7 \times 11)b_3 \equiv 1 \pmod{13} \iff -b_3 \equiv 1 \pmod{13} \iff b_3 \equiv -1 \pmod{13} \end{cases}$$

and  $x \equiv 143 \times 5 \times 2 + 91 \times 4 \times 3 + 77 \times (-1) \times 4 \equiv 212 \pmod{1001}$ . Thus the 2 solutions are 212 and 1213. □

**Proof of Exercise 32.** Another exercise on the CRT. Answer:  $x \equiv 446 \pmod{1122}$ . □

**Proof of Exercise 36.** The idea is to transform the given equations to the form “ $x \equiv \dots$ ”. So, using the fact that  $5^{-1} \equiv 2 \pmod{9}$ , we have  $5x \equiv 2 \pmod{9} \iff x \equiv 2 \times 2 = 4 \pmod{9}$ . Similarly, we get  $x \equiv 9 \pmod{13}$  and  $x \equiv 8 \pmod{17}$ . 9, 13, and 17 are coprime so we can apply the CRT. The solution is  $x \equiv 841 \pmod{1989}$ . □

**Proof of Exercise 38.** Let  $x$  be the number of coins. Then we have  $x \equiv 0 \pmod{78}$  and  $x + 50 \equiv 0 \pmod{77}$ , i.e.  $x \equiv 27 \pmod{77}$ . Using the CRT, we get  $x = 2106$  as the smallest possible number of coins. □

**Proof of Exercise 41.** Solution 1: As in the hint, solve the given quadratic for  $x$  to get  $x = \frac{-y \pm \sqrt{y^2 + 4(y^2 + 3)}}{2}$ . If  $x, y \in \mathbb{Z}$  then the expression under the square root must be the square of an integer, call it  $z$ . So we have  $5y^2 + 12 = z^2$  for some  $z \in \mathbb{Z}$ . But then this equality must hold (mod  $m$ ) for any integer  $m$ . Consider  $m = 5$ . Then we get  $z^2 \equiv 2 \pmod{5}$ , which is impossible (see previous homework or just work out the possible squares (mod 5)). Thus no such  $z$  exists and hence no  $x, y \in \mathbb{Z}$  satisfying the original equation.

Solution 2: Consider the equation (mod 3). So  $x^2 + xy - y^2 \equiv 0 \pmod{3}$ . Now suppose  $x \equiv 0 \pmod{3}$ . Then we get  $y^2 \equiv 0$ , and hence  $y \equiv 0 \pmod{3}$ . But then, working again over the (regular) integers we would get that 9 divides  $x^2 + xy - y^2$ , but certainly it cannot divide 3, contradiction. Similarly we cannot have  $y \equiv 0 \pmod{3}$ , so  $x, y \equiv 1$  or  $2 \pmod{3}$ , i.e.  $x^2 \equiv y^2 \equiv 1 \pmod{3}$  and hence  $xy \equiv 0 \pmod{3}$ , which is again impossible. □

## 2. CHAPTER 3: FERMAT AND WILSON

**Exercises (p. 94):** 1, 3, 5, 11, 12, 13.

**Proof of Exercise 1.** 29 is prime, so  $28! \equiv -1 \pmod{29}$  by Wilson's theorem. Thus  $-1 \equiv 28 \times 27 \times 26 \times 25 \times 24! \equiv (-1)(-2)(-3)(-4)24! \equiv 24 \times 24! \equiv (-5)24!$ , which implies that  $24! = 5^{-1} = 6 \pmod{29}$ .  $\square$

**Proof of Exercise 3.** Multiplying each side of the equation by 1992, we get that  $1992! \equiv -1 \pmod{1993}$ . The result now follows by the converse to Wilson's theorem (see problem 3-20).  $\square$

**Proof of Exercise 5.**  $899 = 29 \times 31$ , and both factors are prime. Let  $x = 27!$ . We need to compute the residues of  $x \pmod{p}$  for each prime  $p$  and then use the CRT to find the residue mod  $29 \times 31 = 899$ . Using Wilson's theorem, we get  $x \equiv 1 \pmod{29}$  and  $x \equiv -5 \pmod{31}$  and by the CRT,  $x \equiv 88 \pmod{899}$ .  $\square$

**Proof of Exercise 11.** To start with,  $54 \equiv 2$  and  $69 \equiv 4 \pmod{13}$ . Then, using Fermat's theorem (certainly 13 is prime and does not divide 2 or 5), we get  $54^{103} + 69^{67} \equiv (2^{12})^8 \times 2^7 + (4^{12})^5 \times 4^7 \equiv 2^7 + 2^{14} \equiv \dots \equiv 2 \pmod{13}$ . Therefore, 13 does not divide the given expression.  $\square$

**Proof of Exercise 12.** By Fermat,  $x^{199} \equiv x \pmod{199}$  for any  $x \in \mathbb{Z}$ . Note that " $x^{198} \equiv 1 \pmod{199}$  for any  $x \in \mathbb{Z}$ " would be incorrect (why?). So we get  $x^2 - x \equiv 0 \pmod{199}$  which has 0 and 1 and its only solutions mod 199). The fact that any degree  $n$  polynomial has at most  $n$  solutions mod a prime  $p$  is Thm. (4.6). What could happen if  $p$  isn't prime?  $\square$

**Proof of Exercise 13.** Suppose  $p = 2$ . Then  $2^p + 1 = 5$ , which is not a multiple of 2. For  $p \neq 2$ ,  $2^p \equiv 2 \pmod{p}$  by Fermat, so  $2^p + 1 \equiv 3 \pmod{p}$ . Thus  $p \mid 2^p + 1 \iff p = 3$ .  $\square$

## 3. ADDITIONAL EXERCISES

**Proof of "Five Pirates and a Monkey".** Let  $x$  be the number of coconuts.

First Pirate. The problem states that  $x \equiv 1 \pmod{5}$  and so there is  $k_1$  such that  $x - 1 = 5k_1$ . Thus,  $4k_1$  coconuts are left after the first pirate leaves.

Second Pirate. It turns out  $4k_1 \equiv 1 \pmod{5}$ , thus  $k_1 \equiv 4 \pmod{5}$  and so there is  $k_2$  such that  $k_1 = 4 + 5k_2$ . Thus,  $4k_1 - 1 = 15 + 20k_2$  and  $\frac{4}{5}(15 + 20k_2) = 12 + 16k_2$  coconuts remain after the second pirate goes.

Third Pirate.  $12 + 16k_2 \equiv 1 \pmod{5}$  and so  $16k_2 \equiv -11 \pmod{5}$ , or  $k_2 \equiv -1 \pmod{5}$ . Hence, there is  $k_3$  such that  $k_2 = 4 + 5k_3$ . Thus,  $(12 + 16k_2) - 1 = 11 + 16(4 + 5k_3) = 80k_3 + 75$  and  $\frac{4}{5}(80k_3 + 75) = 60 + 64k_3$  coconuts remain after the third pirate goes.

Fourth Pirate.  $60 + 64k_3 \equiv 1 \pmod{5}$  and so  $64k_3 \equiv -59 \pmod{5}$ , or  $-k_3 \equiv 1 \pmod{5}$ . Hence, there is  $k_4$  such that  $k_3 = 4 + 5k_4$ . Thus,  $(60 + 64k_3) - 1 = 59 + 64(4 + 5k_4) = 320k_4 + 315$  and  $\frac{4}{5}(320k_4 + 315) = 252 + 256k_4$  coconuts remain after the fourth pirate goes.

Fifth Pirate.  $252 + 256k_4 \equiv 1 \pmod{5}$  and so  $256k_4 \equiv -251 \pmod{5}$ , or  $k_4 \equiv -1 \pmod{5}$ . Hence, there is  $k_5$  such that  $k_4 = 4 + 5k_5$ . Thus,  $(252 + 256k_4) - 1 = 251 + 256(4 + 5k_5) = 1280k_5 + 1275$  and  $\frac{4}{5}(1280k_5 + 1275) = 1020 + 1024k_5$  coconuts remain after the fifth pirate goes.

Final round.  $1020 + 1024k_5 \equiv 1 \pmod{5}$  and so  $1024k_5 \equiv -1019 \pmod{5}$ , or  $k_5 \equiv -1 \pmod{5}$ . Hence, there is  $k_6$  such that  $k_5 = 4 + 5k_6$ . Thus,  $(1020 + 1024k_5) - 1 = 1019 + 1024(4 + 5k_6) = 5120k_6 + 5115$ .

Now, the smallest number will be when  $k_6 = 0$ , and  $k_5 = 4$  and  $k_4 = 4 + 5 \cdot 4 = 24$  and  $k_3 = 4 + 5 \cdot 24 = 124$  and  $k_2 = 4 + 5 \cdot 124 = 624$  and  $k_1 = 4 + 5 \cdot 624 = 3124$  and  $x = 1 + 5 \cdot 3124 = 15621$ .

□

## (2) - 'Day of the Week' problems from Ch. 2.

**Proof of Exercise 43.** As in section (2.12), we find the day of the week for October 12, 1492 (Julian calendar): the 'Julian correction' is  $18 - 14 = 4$ , the year code is  $92 + \lfloor 92/4 \rfloor \equiv 3 \pmod{7}$ , and the month code is 1. Thus the day is  $12 + 4 + 3 + 1 \equiv 6 \pmod{7}$ , a Friday. □

**Proof of Exercise 45.** This is done in the same way as the previous exercise (except for the 'Julian correction'). □

**Proof of (3.1).** To begin with, we must check that our set  $U_m$  is closed under the given operation, i.e. whether for  $a, b \in U_m, ab \in U_m$  as well.  $a \in U_m \Rightarrow \exists a^{-1} \in U_m$  s.t.  $aa^{-1} \equiv 1 \pmod{m}$  and similarly for  $b$ . Then  $(ab)(a^{-1}b^{-1}) = (aa^{-1})(bb^{-1}) \equiv 1 \times 1 = 1 \pmod{m}$  so indeed  $ab \in U_m$ . Note that we are using the fact that multiplication in  $\mathbb{Z}/m\mathbb{Z}$  is commutative. Without assuming that, we would have to write the inverse of  $ab$  as  $b^{-1}a^{-1}$ , etc.

(a) multiplication in  $\mathbb{Z}/m\mathbb{Z}$  is associative, hence so is multiplication in  $U_m$ ;

(b) clearly  $a \times 1 = 1 \times a = a$  in  $\mathbb{Z}/m\mathbb{Z}$ , so we just need to show  $1 \in U_m$ . That's simple enough, since  $1^{-1} = 1$  in  $\mathbb{Z}/m\mathbb{Z}$ ;

(c) each element in  $U_m$  has an inverse in  $U_m$  by the very definition of the set, so we're done. □

**Proof of (3.2).** This stuff will become much clearer in Chapter 6. For now, we can check that 3 and 5 are the primitive roots (mod 7), 2, 6, 7, 8 the primitive roots (mod 11) and 2, 6, 7, 11 the ones (mod 13). Some patterns should have emerged, e.g. if  $g$  is a primitive root, then so is  $g^{-1}$ , if the order of  $U_m$  is  $k = \phi(m)$ , then the 'order' of each element will divide  $k$ , etc.