

# **MAT2120 Number Theory**

## **Problems II**

Suhyun Park (20181634)

Department of Computer Science and Engineering, Sogang University

1. Find all solutions of  $87x \equiv 57 \pmod{105}$ .

*Solution.*

$$87x \equiv 57 \pmod{105} \Leftrightarrow 29x \equiv 19 \pmod{35}.$$

Using the extended Euclidean algorithm to find  $a, b$  that satisfies  $29a + 35b = (29, 35) = 1$  yields

$$\begin{aligned} 35 &= \underline{29} \cdot 1 + \underline{6} \\ 29 &= \underline{6} \cdot 4 + \underline{5} \\ 6 &= \underline{5} \cdot 1 + \underline{1} \\ 5 &= 1 \cdot 5 \\ \therefore 1 &= 6 - 5 \cdot 1 \\ &= 6 - (29 - 6 \times 4) \cdot 1 = 6 \times 5 - 29 \\ &= (35 - 29 \cdot 1) \times 5 - 29 = 35 \times 5 - 29 \times 6 \\ &\Rightarrow a = -6, b = 5. \end{aligned}$$

Hence,

$$\begin{aligned} 19(29a + 35b) &= 19 \times 1 \Rightarrow 19a \times 29 = 19 - 35b \\ &\Rightarrow 19a \times 29 \equiv 19 \pmod{35} \\ 29 \times (-114) &\equiv 19 \pmod{35}. \end{aligned}$$

Thus  $x \equiv -114 \equiv 26 \pmod{35}$ , so  $x \equiv 26$  or  $x \equiv 61$  or  $x \equiv 96$  modulo 105.

2. Show that  $n(n-1)(2n-1)$  is divisible by 6 for every positive integer  $n$ .

*Proof.* Suppose  $n = 6k + r$  where  $k \in \mathbb{Z}$  and  $0 \leq r < 6$  and  $r \in \mathbb{Z}$ . Then

$$\begin{aligned} n(n-1)(2n-1) &= (6k+r)(6k+r-1)(12k+2r-1) \\ &\equiv r(r-1)(2r-1) \\ &\equiv 2r^3 - 3r^2 + r \pmod{6}. \end{aligned}$$

1. Suppose  $r = 2q_2 + r_2$  where  $q_2, r_2 \in \mathbb{Z}$  and  $0 \leq r_2 < 2$ . Then

$$\begin{aligned} 2r^3 - 3r^2 + r &\equiv r^2 + r \\ &\equiv (2q_2 + r_2)^2 + (2q_2 + r_2) \\ &\equiv r_2^2 + r_2 \equiv r_2(r_2 + 1) \pmod{2}. \end{aligned}$$

Since  $0(0+1) \equiv 1(1+1) \equiv 0 \pmod{2}$ ,  $2 \mid n(n-1)(2n-1)$ .

2. Similarly, suppose  $r = 3q_3 + r_3$  where  $q_3, r_3 \in \mathbb{Z}$  and  $0 \leq r_3 < 3$ . Then

$$\begin{aligned} 2r^3 - 3r^2 + r &\equiv 2r^3 + r \\ &\equiv 2(3q_3 + r_3)^3 + (3q_3 + r_3) \\ &\equiv 2r_3^3 + r_3 \equiv r_3(2r_3^2 + 1) \pmod{3}. \end{aligned}$$

Since  $0(2 \cdot 0^2 + 1) \equiv 1(2 \cdot 1^2 + 1) \equiv 2(2 \cdot 2^2 + 1) \equiv 0 \pmod{3}$ ,  $3 \mid n(n-1)(2n-1)$ .

By 1. and 2.,  $2 \times 3 = 6 \mid n(n-1)(2n-1)$  for any integer  $n$ .

3. What are the remainders when  $3^{40}$  and  $43^{37}$  are divided by 11?

*Solution.*

1. By Fermat's Little Theorem,  $3^{11-1} \equiv 1 \pmod{11}$ . Hence

$$\begin{aligned} 3^{40} &\equiv (3^{10})^4 \\ &\equiv 1^4 \equiv 1 \pmod{11}. \end{aligned}$$

2. Note that  $43 \equiv -1 \pmod{11}$ . Thus

$$\begin{aligned} 43^{37} &\equiv (-1)^{37} \\ &\equiv -1 \equiv 10 \pmod{11}. \end{aligned}$$

4. Find all solutions to the pair of congruences  $3x - 7y \equiv 4 \pmod{15}$ ,  $7x - 3y \equiv 1 \pmod{15}$ .

*Solution.* Since

$$\begin{aligned}
 (3x - 7y) \times 3 - (7x - 3y) \times 7 &\equiv 4 \times 3 - 1 \times 7 = 5 \pmod{15} \\
 \Rightarrow 9x - 21x - 49x + 21y &\equiv 5 \pmod{15} \\
 \Rightarrow -40x \equiv 5x &\equiv 5 \pmod{15} \\
 \Rightarrow x &\equiv 1 \pmod{3} \\
 \Rightarrow x &\equiv 1 + 5k \pmod{15}
 \end{aligned}$$

where  $k \in \mathbb{Z}$ ,

$$\begin{aligned}
 3x - 7y &\equiv 4 \pmod{15} \\
 \Rightarrow 3(1 + 5k) - 7y &\equiv 4 \pmod{15} \\
 \Rightarrow 3 + 15k - 7y &\equiv 4 \pmod{15} \\
 \Rightarrow 8y &\equiv 1 \pmod{15}.
 \end{aligned}$$

Thus  $x \equiv 1 \pmod{3}$  and  $y \equiv 2 \pmod{15}$ .

5. Find all integers between 3000 and 5000 that leave remainders of 1, 3, and 5 when divided by 7, 11, and 13, respectively.

*Solution.* Let  $x$  be an integer such that

$$\begin{cases} x \equiv 1 \pmod{7} \\ x \equiv 3 \pmod{11} \\ x \equiv 5 \pmod{13} \end{cases}$$

We derive  $x$  by using the Chinese remainder theorem. Note that the solution of

$$\begin{aligned}
 11 \times 13 \times m_1 &\equiv 3m_1 \equiv 1 \pmod{7} \\
 7 \times 13 \times m_2 &\equiv 3m_2 \equiv 3 \pmod{11} \\
 7 \times 11 \times m_3 &\equiv -m_3 \equiv 5 \pmod{13}
 \end{aligned}$$

is given by  $m_1 \equiv 5 \pmod{7}$ ,  $m_2 \equiv 1 \pmod{11}$ ,  $m_3 \equiv -5 \pmod{13}$ , thus

$$x \equiv 5 \cdot 11 \cdot 13 + 1 \cdot 7 \cdot 13 - 5 \cdot 7 \cdot 11 \equiv 421 \pmod{1001}.$$

Hence integers between 3000 and 5000 that leave remainders of 1, 3, and 5 when divided by 7, 11, and 13 are:

$$3424, 4425.$$

6. Find the remainder when  $13 \cdot 12^{45}$  is divided by 47.

*Solution.*  $13 \cdot 12^{45} = 12^{46} + 12^{45}$ . By Fermat's little theorem,  $12^{47-1} \equiv 1 \pmod{47}$ . Hence

$$\begin{aligned} 13 \cdot 12^{45} &= 12^{46} + 12^{45} \equiv 1 + 12^{45} \\ &\equiv 1 + (12^2)^{22} \times 12 \equiv 1 + (47 \times 3 + 3)^{22} \times 12 \\ &\equiv 1 + 3^{22} \times 12 \\ &\equiv 1 + (3^5)^4 \times 9 \times 12 \equiv 1 + (47 \times 5 + 8)^4 \times 108 \\ &\equiv 1 + 8^4 \times (47 \times 2 + 14) \equiv 1 + 8^4 \times 14 \\ &\equiv 1 + (8^2)^2 \times 14 \equiv 1 + (47 + 17)^2 \times 14 \\ &\equiv 1 + 17^2 \times 14 \\ &\equiv 4047 \equiv 5. \end{aligned}$$

7. Let  $p$  and  $q$  be distinct odd primes such that  $p - 1$  divides  $q - 1$ . If  $(a, pq) = 1$ , prove that  $a^{q-1} \equiv 1 \pmod{pq}$ .

*Proof.* By Fermat's theorem, it is clear that  $a^{q-1} \equiv 1 \pmod{q}$  and  $a^{p-1} \equiv 1 \pmod{p}$ .

Since  $(p - 1) \mid (q - 1)$ , we can let  $(q - 1) = k(p - 1)$ , where  $2 \leq k$  and  $k \in \mathbb{Z}$ . Then

$$\begin{aligned} (a^{p-1})^k &\equiv 1^k \equiv 1 \pmod{p} \\ \Rightarrow a^{k(p-1)} &\equiv 1 \pmod{p} \\ \Rightarrow a^{q-1} &\equiv 1 \pmod{p}. \end{aligned}$$

Since  $p$  and  $q$  are distinct primes; i. e.  $(p, q) = 1$ , and since  $a^{q-1}$  is congruent to 1 both modulo  $p$  and  $q$ ,  $a^{q-1} \equiv 1 \pmod{pq}$ .  $\square$

8. Show that if  $a$  is not divisible by 2 or by 5, then  $a^{101}$  ends in the same three decimal digits as does  $a$ . (Here we use the convention that 21, for example, ends with 021.)

*Proof.* We want to show that  $a^{101} \equiv a \pmod{1000}$ .

Since  $a$  is not divisible by 2 nor 5 but the only prime factor of 125 is 5,  $(a, 125) = 1$ . Note that

$$\begin{aligned}\phi(125) &= 125 \left(1 - \frac{1}{5}\right) \\ &= 100.\end{aligned}$$

By Euler's theorem,  $a^{\phi(125)} = a^{100} \equiv 1 \pmod{125}$ .

Also for 8, since only prime factor of 8 is 2 and  $\phi(8) = 4$ , By Euler's theorem,  $a^{\phi(8)} = a^4 \equiv 1 \pmod{8}$ . Hence,  $(a^4)^{25} \equiv a^{100} \equiv 1 \pmod{8}$ .

Thus since  $(8, 125) = 1$ ,  $a^{100} \equiv 1 \pmod{1000}$ ; therefore  $a^{101} \equiv a \pmod{1000}$ .  $\square$

9. Explain why every year has at least one Friday the 13<sup>th</sup>.

*Proof.* If January begins on day  $k$ , where  $0 \leq k < 7$  and  $k = 0$  being Sunday, then on a non-leap year,

- February begins on day  $k + 31 \equiv k + 3 \pmod{7}$
- March begins on day  $k + 3 + 28 \equiv k + 3 \pmod{7}$
- April begins on day  $k + 3 + 31 \equiv k + 6 \pmod{7}$
- May begins on day  $k + 6 + 30 \equiv k + 1 \pmod{7}$
- June begins on day  $k + 1 + 31 \equiv k + 4 \pmod{7}$
- July begins on day  $k + 4 + 30 \equiv k + 6 \pmod{7}$
- August begins on day  $k + 6 + 31 \equiv k + 2 \pmod{7}$
- September begins on day  $k + 2 + 31 \equiv k + 5 \pmod{7}$
- October begins on day  $k + 5 + 30 \equiv k \pmod{7}$
- November begins on day  $k + 31 \equiv k + 3 \pmod{7}$
- December begins on day  $k + 3 + 30 \equiv k + 5 \pmod{7}$

Then the set of starting days of each month forms a complete residue system, hence the set of days of the 13<sup>th</sup> of each month also does. Similarly, this also holds in leap years. Thus it is guaranteed that every year will have at least one Friday the 13<sup>th</sup>.