Дискрет мат, Семинар №10

1. Батал.

1. $a \equiv a \pmod m$
2. $a \equiv b \pmod m$ бол $b \equiv a \pmod m$
3. $a \equiv b \pmod m$, $b \equiv c \pmod m$ бол $a \equiv c \pmod m$
4. $a \equiv b \pmod m \Leftrightarrow a, b$ нь m-д хуваахад адил үлдэгдэл өгнө. Энд $b = 0$ гэвэл $a \equiv 0 \pmod m \Leftrightarrow m \mid a$ болно.
5. $a \equiv 0 \pmod m$, $a \equiv 0 \pmod n$ бол $a \equiv 0 \pmod{[n, m]}$
6. $b \equiv 0 \pmod m$, $a \equiv 0 \pmod n$ бол $ab \equiv 0 \pmod{mn}$ байна.
7. $a \equiv b \pmod m$, $d \mid m$ бол $a \equiv b \pmod d$
8. $a \equiv b \pmod m \Leftrightarrow (a, m) = (b, m)$

Бодолт 1.
Заавар: $a \equiv b \pmod m \Leftrightarrow m \mid a - b$
Бодолт:

1. $a \equiv a \pmod m$
2. $a \equiv b \pmod m$ бол $b \equiv a \pmod m$
3. $a \equiv b \pmod m$, $b \equiv c \pmod m$ бол $a \equiv c \pmod m$
   $m \mid a - b$, $m \mid b - c \Rightarrow m \mid (a - b) + (b - c) = a - c$
4. $a \equiv b \pmod m \Leftrightarrow a, b$ нь m-д хуваахад адил үлдэгдэл өгнө. Энд $b = 0$ гэвэл $a \equiv 0 \pmod m \Leftrightarrow m \mid a$ болно.
5. $a \equiv 0 \pmod m$, $a \equiv 0 \pmod n$ бол $a \equiv 0 \pmod{[n, m]}$
6. $b \equiv 0 \pmod m$, $a \equiv 0 \pmod n$ бол $ab \equiv 0 \pmod{mn}$ байна.
7. $a \equiv b \pmod m$, $d \mid m$ бол $a \equiv b \pmod d$
8. $a \equiv b \pmod m \Leftrightarrow (a, m) = (b, m)$

2. $+_7$, $\cdot_7$, $+_{12}$, $\cdot_{12}$-ийн хүснэгтийг байгуул.
Бодолт 1.
Заавар:
Бодолт:

$+_7$	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

$\cdot_7$	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

$+_{12}$	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11	0
2	2	3	4	5	6	7	8	9	10	11	0	1
3	3	4	5	6	7	8	9	10	11	0	1	2
4	4	5	6	7	8	9	10	11	0	1	2	3
5	5	6	7	8	9	10	11	0	1	2	3	4
6	6	7	8	9	10	11	0	1	2	3	4	5
7	7	8	9	10	11	0	1	2	3	4	5	6
8	8	9	10	11	0	1	2	3	4	5	6	7
9	9	10	11	0	1	2	3	4	5	6	7	8
10	10	11	0	1	2	3	4	5	6	7	8	9
11	11	0	1	2	3	4	5	6	7	8	9	10

$\cdot_{12}$	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	1	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	1	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	1

3. Дараах тохиолдлуудад $a\mathbb{Z}_m$

1. $a = 2$, $m = 7$
2. $a = 3$, $m = 16$
3. $a = 3$, $m = 15$
4. $a = 16$, $m = 103$
5. $a = 12$, $m = 21$

Бодолт 1.

Заавар:

Бодолт:

1. $a = 2$, $m = 7$ тохиолдолд
$$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$$
ба
$$\begin{aligned} 2\mathbb{Z}_7 &= \{2 \cdot_7 0, 2 \cdot_7 1, 2 \cdot_7 2, 2 \cdot_7 3, 2 \cdot_7 4, 2 \cdot_7 5, 2 \cdot_7 6\} \\ &= \{0, 2, 4, 6, 1, 3, 5\} = \mathbb{Z}_7 \end{aligned}$$
байна.

2. $a = 3$, $m = 16$ тохиолдолд
$$\mathbb{Z}_{16} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15\}$$
ба
$$\begin{aligned} 3\mathbb{Z}_{16} &= \{3 \cdot 0, 3 \cdot 1, 3 \cdot 2, 3 \cdot 3, 3 \cdot 4, 3 \cdot 5, 3 \cdot 6, 3 \cdot 7, 3 \cdot 8, 3 \cdot 9, 3 \cdot 10, 3 \cdot 11, 3 \cdot 12, 3 \cdot 13, 3 \cdot 14, 3 \cdot 15\} \\ &= \{0, 3, 6, 9, 12, 15, 2, 5, 8, 11, 14, 1, 4, 7, 10, 13\} = \mathbb{Z}_{16} \end{aligned}$$
байна. Энд $\cdot = \cdot_{16}$ юм.

3. $a = 3$, $m = 15$ тохиолдолд
$$\mathbb{Z}_{15} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$$
ба
$$\begin{aligned} 3\mathbb{Z}_{15} &= \{3 \cdot 0, 3 \cdot 1, 3 \cdot 2, 3 \cdot 3, 3 \cdot 4, 3 \cdot 5, 3 \cdot 6, 3 \cdot 7, 3 \cdot 8, 3 \cdot 9, 3 \cdot 10, 3 \cdot 11, 3 \cdot 12, 3 \cdot 13, 3 \cdot 14\} \\ &= \{0, 3, 6, 9, 12, 0, 3, 6, 9, 12, 0, 3, 6, 9, 12\} \neq \mathbb{Z}_{15} \end{aligned}$$
байна. Энд $\cdot = \cdot_{15}$ юм.

4. $a = 16$, $m = 103$. $(16, 103) = 1$ тул $\exists 16^{-1} \pmod{103}$ байна. Иймд $\forall b \in \mathbb{Z}_{103}$-ийн хувьд
$$16x \equiv b \pmod{103} \Leftrightarrow x \equiv 16^{-1} b \pmod{103}$$
байх тул $b \in 16\mathbb{Z}_{103}$ болно. Өөрөөр хэлбэл $\mathbb{Z}_{103} \subseteq 16\mathbb{Z}_{103}$. Нөгөө талаас $16\mathbb{Z}_{103} \subseteq \mathbb{Z}_{103}$ байх нь тодорхойлолт ёсоор илэрхий юм.

5. $a = 12$, $m = 21$ тохиолдолд $\mathbb{Z}_{21} \neq 12\mathbb{Z}_{21}$ байна. Учир нь $(12, 21) = 3 > 1$ тул
$$12 \cdot 0 \equiv 12 \cdot 7 \equiv 12 \cdot 14 \equiv 0 \pmod{21}$$
буюу $|12\mathbb{Z}_{21}| < 21 = |\mathbb{Z}_{21}|$ байна. Үнэндээ
$$12\mathbb{Z}_{21} \equiv \{0, 3, 6, 9, 12, 15, 18\}$$
юм.

4. Дараах тэгшитгэлийг бод.

1. $15 \cdot_{16} x -_{16} 7 = 0$
2. $19 \cdot_{13} x -_{13} 3 = 0$
3. $15 \cdot_{18} x -_{18} 6 = 0$
4. $16 \cdot_{32} x -_{32} 2 = 0$

Бодолт 1.

Заавар:

Бодолт:

1. $15 \cdot_{16} x -_{16} 7 = 0 \Rightarrow 15x \equiv 7 \pmod{16}$ байна. $15 \equiv -1 \pmod{16}$ тул
$$15^{-1} \equiv (-1) \equiv 15 \pmod{16}$$
юм. Иймд $15x \equiv 7 \pmod{16} \Rightarrow 15 \cdot (15x) \equiv 15 \cdot 7 \pmod{16}$ буюу $x \equiv 9 \pmod{16}$ тул $x = 9$ байна.
2. $19 \cdot_{13} x -_{13} 3 = 0$. $19 \cdot 2 \equiv -1 \pmod{13}$ тул $19^{-1} \equiv -2 \pmod{13}$ тул $19^{-1} =_{13} 11$ байна. Өгсөн тэгшитгэлийг 11-ээр үржүүлбэл
$$11 \cdot_{13} (19 \cdot_{13} x) - 11 \cdot_{13} 3 = 0 \Leftrightarrow (19^{-1} \cdot_{13} 19) \cdot_{13} x - 7 = 0$$
буюу $x = 7$ болно.
3. $15 \cdot_{18} x -_{18} 6 = 0$ тэгшитгэлийн хувьд $(15, 18) = 3$ тул 18 модулаар $x = 15^{-1}$ буюу $15x \equiv 1 \pmod{18}$ байх тоо оршин байхгүй. Иймд өмнөхтэй ижил урвуугаар үржүүлж бодох боломжгүй юм. Харин
$$15 \cdot_{18} x -_{18} 6 = 0 \Rightarrow 15x - 18y = 6 \equiv 5x - 6y = 2$$
хэлбэрт бичээд 6 модулаар бодвол $x = -2$, $y = -2$ буюу $x = 6k - 2$ хэлбэрийн шийдтэй болох нь харагдаж байна. Эндээс $k = 1, 2, 3$ үед $x = 4$, $x = 10$, $x = 16$ гэсэн гурван шийд $\mathbb{Z}_{18}$-д байна.
4. $16 \cdot_{32} x -_{32} 2 = 0$ тэгшитгэл шийд. Эсрэгээс нь шийдтэй гэвэл $16x - 32y = 2$ байх y тоо оршин байх шаардлагатай. Гэвч тэнцэлийн зүүн гар тал нь 16-д хуваагдах тоо, баруун гар талд 16-д хуваагдахгүй тоо гарч тул зөрчил үүсч байна. Иймд шийдгүй тэгшитгэл юм.

5. $199 \cdot 1111$-ийг $\mathbb{Z}_{1176}$-д тооцоол. $(23^{1111})^{199}$, $(105^{1111})^{199}$-ийг $\mathbb{Z}_{1247}$-д тооцоол.

Бодолт 1.

Заавар: $p \in \mathbb{P}$ (анхны тоо). $(a, p) = 1$ бол
$$a^{p-1} \equiv 1 \pmod{p}$$
Фермагийн теорем.

Бодолт: $199 \cdot 1111 = 221089 = 1176 \cdot 188 + 1$ тул $199 \cdot 1111 \equiv 1 \pmod{1176}$. $1247 = 29 \cdot 43$ тул
$$\begin{cases} 23^{28} \equiv 1 \pmod{29} \\ 23^{42} \equiv 1 \pmod{43} \end{cases} \Rightarrow \begin{cases} (23^{28})^{42} \equiv 1 \pmod{29} \\ (23^{42})^{28} \equiv 1 \pmod{43} \end{cases} \Rightarrow \begin{cases} 23^{1176} \equiv 1 \pmod{29} \\ 23^{1176} \equiv 1 \pmod{43} \end{cases}$$
тул $23^{1176} \equiv 1 \pmod{29 \cdot 43 = 1247}$ байна. Иймд
$$(23^{1111})^{199} = 23^{1176 \cdot 188 + 1} \equiv 23 \pmod{1247}$$
байна.

6. 4-ийн зэргүүдийг $\mathbb{Z}_7$, $\mathbb{Z}_{10}$-д тооцоол.

Бодолт 1.

Заавар:

Бодолт: $4^1 = 4$, $4^2 = 4 \cdot_7 4 = 2$, $4^3 = 2 \cdot_7 4 = 1$, $4^4 = 1 \cdot_7 4 = 4$ гэх мэтчилэн $n = 3k$ үед $4^n = 1$, $n = 3k+1$ үед $4^n = 4$, $n = 3k+2$ үед $4^{3k+2} = 2$ байна.

$4^1 = 4$, $4^2 = 4 \cdot_{10} 4 = 6$, $4^3 = 6 \cdot_{10} 4 = 4$, $4^4 = 4 \cdot_{10} 4 = 6$ гэх мэтчилэн n тэгш үед 6, n сондгой тоо үед 4 байна.

7. $\{1 \cdot_{11} 5, 2 \cdot_{11} 5, \ldots, 10 \cdot_{11} 5\}$-ийг тооцоол. Хэрэв 5-ийн оронд $\mathbb{Z}_{11}$-ийн өөр элемент авбал $\{1, 2, \ldots, 10\}$ гарах уу?

8. $\begin{cases} x \equiv 4 \pmod 5 \\ x \equiv 5 \pmod 7 \end{cases}$ систем $\{0, 1, \ldots, 34\}$ дээр нийт хэдэн шийдтэй вэ? Шийдийг ол.

Бодолт 1.

Заавар:

Бодолт: $x \equiv 4 \pmod 5$ тул $x = 5k+4$ хэлбэртэй байна. Эндээс $5k + 4 \equiv 5 \pmod 7$ тул $5k \equiv 1 \pmod 7$ болно. Шууд шалгах замаар $k \equiv 3 \pmod 7$ болохыг харж болно. Эндээс $k = 7t + 3$ болно. Иймд

$$x = 5k + 4 = 5(7t + 3) + 4 = 35t + 19$$

$\{0, 1, \ldots, 34\}$ байх шийд нь зөвхөн $t = 0$ үед $x = 19$ юм.

9. Тооны машин компьютер ашиглахгүйгээр

1. $15^{96}, 15^{200}$-г $\mathbb{Z}_{97}$-д ол.
2. $67^{73}, 67^{200}$-г $\mathbb{Z}_{73}$-д ол.

Бодолт 1.

Заавар: Фермагийн теоремоор $(a, p) = 1$, p анхны тоо бол

$$a^{p-1} \equiv 1 \pmod p$$

байдаг.

Бодолт:

1. 97 анхны тоо ба $(15, 97) = 1$ тул Фермагийн теоремоор
$$15^{96} \equiv 15^{97-1} \equiv 1 \pmod{97},$$
$$15^{200} \equiv 15^{2 \cdot 96 + 4} \equiv 15^4 \equiv 225^2 \equiv 31^2 \equiv 961 \equiv 89 \pmod{97}$$
байна.
2. 73 анхын тоо ба $(67, 73) = 1$ тул Фермагийн теоремоор
$$67^{73} \equiv 67 \pmod{73},$$
$$\begin{aligned} 67^{200} &\equiv 67^{2 \cdot 72 + 56} \equiv 67^{56} && \pmod{73} \\ &\equiv ((-6)^4)^{14} \equiv (-18)^{14} && \pmod{73} \\ &\equiv ((-18)^2)^7 \equiv 32^7 && \pmod{73} \\ &\equiv 32 \cdot (32^2)^3 \equiv 32 \cdot 2^3 && \pmod{73} \\ &\equiv 37 && \pmod{73} \end{aligned}$$

10. p анхны тоо байг.

1. $\mathbb{Z}_{p^2}$-д урвуутай элемент $p^2 - p$ ширхэг байгаа гэж харуул.
2. Хэрэв x урвуутай элемент бол $x^{p^2-p} \equiv ? \pmod{p^2}$
3. Хэрэв x урвуугүй элемент бол өмнөх өгүүлбэр үнэн үү?

Бодолт 1.

Заавар:

Бодолт:

1. a тоо p^2 модулаар урвуутай байх зайлшгүй бөгөөд хүрэлцээтэй нөхцөл нь $(a, p^2) = (a, p) = 1$ байна. Нөгөө талаас $(a, p) \neq 1$ бол $p \mid a$ ба $\mathbb{Z}_{p^2}$-д p-д хуваагдах тоо $\frac{p^2}{p} = p$ ширхэг байх тул хуваагдахгүй тоо $p^2 - p$ байна. Иймд $\mathbb{Z}_{p^2}$-д урвуутай элементийн тоо $p^2 - p$ ширхэг байна.

2. $\mathbb{Z}^*_{p^2} \subseteq \mathbb{Z}_{p^2}$ нь $\mathbb{Z}_{p^2}$-ийн урвуутай элементүүдийн олонлог бол

$$x\mathbb{Z}^*_{p^2} \equiv \mathbb{Z}^*_{p^2} \pmod{p^2}$$

байна. Учир нь $\forall a, b \in \mathbb{Z}^*_{p^2}$ элементийн хувьд $(ab)^{-1} \equiv a^{-1}b^{-1} \pmod{p^2}$ тул $ab \in \mathbb{Z}^*_{p^2}$ байна. Иймд

$$x\mathbb{Z}^*_{p^2} \subseteq Z^*_{p^2}$$

$$x\mathbb{Z}^*_{p^2} \subseteq \mathbb{Z}^*_{p^2} \pmod{p^2}$$

Нөгөө талаас $\forall b \in \mathbb{Z}^*_{p^2}$ хувьд $b \equiv x \cdot (x^{-1}b) \pmod{p^2}$ ба $x^{-1}b \in \mathbb{Z}^*_{p^2}$ тул $b \in x\mathbb{Z}^*_{p^2}$ буюу

$$\mathbb{Z}^*_{p^2} \subseteq xZ^*_{p^2}$$

болов. Иймд $x\mathbb{Z}^*_{p^2} \equiv \mathbb{Z}^*_{p^2} \pmod{p^2}$ байна. Эдгээр олонлогуудын элементүүдийг үржүүлбэл

$$x^{p^2-p} \prod_{t \in \mathbb{Z}^*_{p^2}} t \equiv \prod_{t \in \mathbb{Z}^*_{p^2}} t \pmod{p^2}$$

тул

$$x^{p^2-p} \prod_{t \in \mathbb{Z}^*_{p^2}} t \prod_{t \in \mathbb{Z}^*_{p^2}} t^{-1} \equiv \prod_{t \in \mathbb{Z}^*_{p^2}} t \prod_{t \in \mathbb{Z}^*_{p^2}} t^{-1} \pmod{p^2}$$

буюу

$$x^{p^2-p} \equiv 1 \pmod{p^2}$$

болно.

3. Худал. Жишээ нь $x = 0$ бол $0^{p^2-p} \not\equiv 1 \pmod{p^2}$ байна.

11. p, q анхны тоонууд бол $\mathbb{Z}_{pq}$-ийн нийт хичнээн элемент урвуутай вэ?
Бодолт 1.
Заавар:
Бодолт: $\exists a^{-1} \Leftrightarrow (a, pq) = 1$ байна. Иймд $a \in \mathbb{Z}_{pq}$ элемент урвуугүй бол $p \mid a$ эсвэл $q \mid a$ байна.

$$A = \{x \mid (x, pq) = p, x \in \mathbb{Z}_{pq}\}$$

$$B = \{y \mid (y, pq) = q, y \in \mathbb{Z}_{pq}\}$$

гэвэл $|A| = \frac{pq}{p} = q$, $|B| = \frac{pq}{q} = p$, $|A \cap B| = \{0\}$ байна. Иймд урвуугүй элементийн тоо

$$|A \cup B| = q + p - 1$$

байна. Харин урвуутай элементүүдийн тоо

$$pq - q - p + 1 = (p-1)(q-1)$$

байна.

12. p, q анхны тоонууд ба $(a, p) = 1, (a, q) = 1$ бол $a^{(p-1)(q-1)} \equiv ? \pmod{pq}$
Бодолт 1.
Заавар: $a\mathbb{Z}^*_{pq} \equiv \mathbb{Z}^*_{pq} \pmod{pq}$ ба $|\mathbb{Z}^*_{pq}| = (p-1)(q-1)$ болохыг ашигла.
Бодолт: $a\mathbb{Z}^*_{pq} \equiv \mathbb{Z}^*_{pq} \pmod{pq}$ тул

$$\prod_{t \in \mathbb{Z}^*_{pq}} (at) \equiv \prod_{t \in \mathbb{Z}^*_{pq}} t \pmod{pq}$$

байна. Үүнийг $\prod_{t \in \mathbb{Z}^*_{pq}} t^{-1}$-ээр үржүүлбэл

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$$

болно.

13. Фермагийн бага теорем дээр p анхны тоо биш үед $a^{p-1} \equiv 1 \pmod p$ байх жишээ, $a^{p-1} \not\equiv 1 \pmod p$ байх жишээ тус тус гарга.

Бодолт 1.

Заавар:

Бодолт: $p = 9$ үед $8^8 \equiv 1 \pmod 9$, $2^8 = 256 \equiv 4 \not\equiv 1 \pmod 9$ байна.

14. RSA-д $p = 11, q = 19, e = 7$ бол d-г ол. 100-г ямар тоо болгон илгээх вэ? Гарсан тооноос хэрхэн 100-г гарган авах вэ?

Бодолт 1.

Заавар:

Бодолт: $(p-1)(q-1) = (11-1)(19-1) = 180$ байна. Түүнчлэн

$$7x - 180y = 1$$

тэгшитгэлийн Эвклидийн алгоритм ашиглан бодвол

$$\begin{aligned} 180 &= 25 \cdot 7 + 5 \\ 7 &= 5 \cdot 1 + 2 \\ 5 &= 2 \cdot 2 + 1 \end{aligned}$$

тул

$$\begin{aligned} 1 &= 1 \times 5 - 2 \times 2 \\ &= 1 \times 5 - 2 \times (7 - 5 \times 1) = 3 \times 5 - 2 \times 7 \\ &= 3 \times (180 - 25 \times 7) - 2 \times 7 = 3 \times 180 - 77 \times 7 \end{aligned}$$

Иймд ерөнхий шийд нь

$$\begin{cases} x = -77 + 180n \\ y = -3 + 7n \end{cases}$$

байна. Эндээс $x \in \mathbb{Z}_{180}$ гэвэл $n = 1$ үед $x = -77 + 180 \cdot 1 = 103$ болно. Иймд $d = 103$. $11 \cdot 19 = 209$ ба

$$100^7 \equiv 111 \pmod{209}$$

тул 100 гэсэн мессежийг 111 болгон илгээнэ. Харин ирсэн 111 мессежийг

$$111^{103} \equiv 100 \pmod{209}$$

гэж буцаана.

15. RSA-д $p = 11, q = 23, e = 13$ бол d-г ол. 100-г ямар тоо болгон илгээх вэ? Гарсан тооноос хэрхэн 100-г гарган авах вэ?

Бодолт 1.

Заавар:

Бодолт: $(p-1)(q-1) = (11-1)(23-1) = 220$ байна. Түүнчлэн

$$13x - 220y = 1$$

тэгшитгэлийн Эвклидийн алгоритм ашиглан бодвол

$$\begin{cases} x = 17 + 220n \\ y = 1 + 13n \end{cases}$$

байна. Эндээс $x \in \mathbb{Z}_{220}$ гэвэл $n = 0$ үед $x = 17 + 180 \cdot 0 = 17$ болно. Иймд $d = 17$. $11 \cdot 23 = 253$ ба

$$100^{13} \equiv 133 \pmod{253}$$

тул 100 гэсэн мессежийг 133 болгон илгээнэ. Харин ирсэн 133 мессежийг

$$133^{17} \equiv 100 \pmod{253}$$

гэж сэргээнэ.