

合同関係

情報通信工学実験B / 電子情報学実験B

電気通信大学 情報理工学域 II類 情報通信工学プログラム/電子情報学プログラム

割り算での余りを考える

- 9を5で割ったときの余り r はいくつ？

$$9 \div 5 = b \cdots r$$

- -9 を5で割ったときの余り r はいくつ？

$$(-9) \div 5 = b \cdots r$$

商と余り

- a, b を整数とし、 $b \geq 0$ とする。そのとき、

$$a = bq + r, \quad 0 \leq r < b$$

を成り立たせる整数 q と r をそれぞれ a を b で割った整商、余り(または剰余)という。

- 特に、 $r = 0$ 、すなわち $a = bq$ となる場合、 a は b で割り切れるという。
- 例えば、 $(a, b) = (13, 5)$ とする。このとき、13 を 5 で割った商と余りは、

$$13 = 5 \times 2 + 3, \quad 0 \leq 3 < 5$$

より、商 2 と余り 3 となる。

商と余り ($a = bq + r$, $0 \leq r < b$)

- $(a, b) = (9, 5)$ とする。このとき、9を5で割った商と余りは、

$$9 = 5 \times 1 + 4, \quad 0 \leq 4 < 5$$

より、商1と余り4となる。

- $(a, b) = (-9, 5)$ とする。このとき、-9を5で割った商と余りは、

$$-9 = 5 \times (-2) + 1, \quad 0 \leq 1 < 5$$

より、商-2と余り1となる。

合同関係

- a, b を整数とするとき、もし $a - b$ が m で割り切れる

(あるいは、 a, b を m で割ったときの余りが等しい)

ならば、

a, b は m を法 (modulo) として(あるいは、法 m に関して)

合同であるといい、

$$a \equiv b \pmod{m}$$

と表す。

練習問題: 以下の式を満たす b の例を挙げよ

- $7 \equiv b \pmod{4}$ 4 で割って余りが 3 になる整数
 - 解: $b = \dots, -9, -5, -1, 3, 7, 11, \dots$
 - $7 = 4 \times 1 + 3$
 - $-9 = 4 \times (-3) + 3$
- $7 \equiv b \pmod{5}$
 - 解: $b =$
 - $7 =$
 - \dots
- $-9 \equiv b \pmod{5}$
 - 解: $b =$
 - $-9 =$
 - \dots

練習問題: 以下の式を満たす b の例を挙げよ

- $7 \equiv b \pmod{4}$ 4 で割って余りが 3 になる整数
 - 解: $b = \dots, -9, -5, -1, 3, 7, 11, \dots$
 - $7 = 4 \times 1 + 3$
 - $-9 = 4 \times (-3) + 3$
- $7 \equiv b \pmod{5}$ 5 で割って余りが 2 になる整数
 - 解: $b = \dots, -13, -8, -3, 2, 7, 12, 17, \dots$
 - $7 = 5 \times 1 + 2$
 - $-8 = 5 \times (-2) + 2$
- $-9 \equiv b \pmod{5}$ 5 で割って余りが 1 になる整数
 - 解: $b = \dots, -14, -9, -4, 1, 6, 11, \dots$
 - $-9 = 5 \times (-2) + 1$
 - $11 = 5 \times 2 + 1$