

1 剰余の定理

$P(a)$ を a に関する多項式とする

$$P(a) = (a - k)Q(a) + R$$

($P(a)$ を $(a - k)$ で割る)

ここで、 $a = k$ を代入すると

$$P(k) = (k - k)Q(k) + R$$

$$P(k) = R = 0$$

$$\text{よって } P(a) = (a - k)Q(a) + P(k)$$

つまり $P(k) = 0 \Leftrightarrow P(a)$ を $(a - k)$ で割り切れる。

具体例

$P(a) = a^n - b^n$ とすると、 $P(b) = b^n - b^n = 0$ なので、 $(a - b)$ は $a^n - b^n$ を割り切れる

実際に、 $a^n - b^n = (a - b)(\sum_{k=0}^{n-1} a^{n-1-k} b^k)$

$n = 3$ のとき、 $a^3 - b^3 = (a - b)(a^2 + ab + b^2)$