2012年6月26日

$$
\begin{aligned}
r_0 &= r_1 q_2 + r_2,\\
r_1 &= r_2 q_3 + r_3,\\
&\vdots\\
r_{n-2} &= r_{n-1} q_n + r_n,\\
r_{n-1} &= r_n q_{n+1}.
\end{aligned}
$$

r_n の作り方から $r_{n+1}=0$ より、r_{n-1} は r_n で割り切れている。r_{n-2} を r_{n-1} で割った余りが r_n であるということから r_{n-2} も r_n で割り切れている。同様に r_{n-3} も r_n で割り切れている。続けていくと r_1, r_0 も r_n で割り切れている。したがって r_n は a,b 両方を割り切っている。

$$
d = \begin{cases} r_n & (A=\mathbb{Z}),\\ r_n \text{ をその最高次の係数で割ったもの} & (A=K[x]) \end{cases}
$$

とおくと、上で示したように、d は a,b 両方を割り切っている。

また、$e|a$ かつ $e|b$ とすると、$e|r_0$ かつ $e|r_1$ である。r_2 は r_0 を r_1 で割った余りなので $e|r_2$ となる。r_3 は r_1 を r_2 で割った余りなので $e|r_1, e|r_2$ より $e|r_3$ となる。同様に続けていくと $e|r_n$ がわかる。よって $e|d$ となる。

以上より、$d=\gcd(a,b)$ が言えた。

例として、

$$
a = 2x^2+x+1,\ b = x^2+3 \in (\mathbb{Z}/5\mathbb{Z})[x]
$$

を考える。

$$
\begin{gathered}
2x^2+x+1 = (x^2+3)2 + x,\\
x^2+3 = x\cdot x + 3.
\end{gathered}
$$

$$
\begin{aligned}
1 &= \frac{3}{3}\\
&= 2\cdot 3\\
&= 2(x^2+3-x\cdot x)\\
&= 2(x^2+3-(2x^2+x+1-2(x^2+3))\cdot x)\\
&= 3x(2x^2+x+1) + 2(2x+1)(x^2+3).
\end{aligned}
$$