ユークリッドの互除法

a，b，q，r が正の整数で，$a=bq+r$ であるとき，a，b の最大公約数と，b，r の最大公約数は一致することを証明せよ。

＜ '05 広島市立大 文字を変更 ＞

【戦略】

ユークリッドの互除法の原理の証明です。

a，b の最大公約数を G とし，b，r の最大公約数を G' とします。

$G=G'$ を示せばよいわけですが，独特の流れで証明します。

大枠の方針としては $G \leqq G'$ かつ $G' \leqq G$ という 2 つが言えれば，$G=G'$ と言えるわけです。

経験がないと中々厳しいでしょう。

【解答】

$a=bq+r$ …① とする。

a，b の最大公約数を G とし，b，r の最大公約数を G' とする。

まず，$\begin{cases} a=G\alpha \\ b=G\beta \end{cases}$ (α，β は互いに素な正整数) と表せる。

① より，$G\alpha=G\beta q+r$ なので，$r=G(\alpha-\beta q)$ であるから

b，r は公約数 G をもつ。

b，r の最大公約数は G' であるから，$G \leqq G'$ …(☆)

一方，$\begin{cases} b=G'u \\ r=G'v \end{cases}$ (u，v は互いに素な正整数) と表せる。

① より，$a=G'uq+G'v$，すなわち $a=G'(uq+v)$ であるから

a，b は公約数 G' をもつ。

a，b の最大公約数は G であるから，$G' \leqq G$ …(★)

(☆)，(★) より $G=G'$ を得る。

以上から a，b の最大公約数と，b，r の最大公約数は一致することが示された。

【総括】

イメージの話をします。

437 と 209 の最大公約数を例にとってみます。

$437=19\cdot 23$ ， $209=19\cdot 11$ なので，19 が最大公約数ですが，数が大きくなってくると「素因数を探す」という態度はつらくなってきます。

「数を小さくする」ということを考えると

$437-209=228\,(=19\cdot 12)$ となり，当然ですが，$19\cdot\bigcirc-19\cdot\triangle$ という形の引き算になるため，結果も 19 の倍数となります。

つまり，437 と 209 の最大公約数は $228\,(=437-209)$ と 209 の最大公約数と同じということです。

引き算しても最大公約数は変化しないということですね。

これを文字で一般化して考えてみます。

－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－

以下，a，b を $a>b$ である正整数とします。

a，b の最大公約数を G としたとき，$\begin{cases} a=G\alpha \\ b=G\beta \end{cases}$（$\alpha$，$\beta$ は互いに素な正整数）

と表せるわけですが，$a-b=G(\alpha-\beta)$ です。

α，β が互いに素であるとき，β と $\alpha-\beta$ も互いに素です。

なぜなら，β，$\alpha-\beta$ が互いに素でないと仮定すると

$$\beta=gK\,,\ \alpha-\beta=gL$$

となるような $g\,(\geqq 2)$ が存在します。

このとき，$\alpha=\beta+gL=g(K+L)$ となり，α，β が公約数 $g\,(\geqq 2)$ をもつことになり，α，β が互いに素であることに矛盾してしまいます。

よって，a，b（$a>b$）の最大公約数と，b，$a-b$ の最大公約数は等しいことになるわけです。

引き算しても最大公約数が変化しないということであれば

a，b（$a>b$）の最大公約数と

$$b \text{ と } \overbrace{a-b-b-\cdots-b}^{q\text{個}}\,(=a-bq)$$

の最大公約数は等しいわけです。（a から b を引けるだけ引いた）

ここまでくると，a を b で割った商を q，余りを r とした

$$a=bq+r$$

とも結びついてくるでしょう。

$a-bq=r$ ですから，a，b の最大公約数と b，r の最大公約数は等しいことになります。