06. GCDを求めるアルゴリズム

代数Ⅱ

ユークリッドの互除法（再）

2つの正整数$a, b (a < b)$において，大きい数bから小さい数aを引いて

$$(a, b) = (a, b - a)$$

2つの正整数$a, b (a < b)$において，大きい数bを数aで整除して

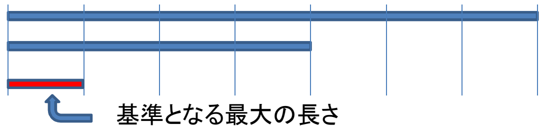
$$b = qa + r$$
$$(a, b) = (a, r)$$

(527,901)＝17

$$\begin{array}{rrrrrr}
 & 4 & 2 & 2 & 1 & 1 \\
17\,) & 68\,) & 153\,) & 374\,) & 527\,) & 901 \\
 & 68 & 136 & 306 & 374 & 527 \\
\hline
 & 0 & 17 & 68 & 153 & 374
\end{array}$$

応用問題

長さa,bの2つの線分に対し，第3の長さcを求め，aとbがそれぞれcの整数倍にできるとき，cをaとbの”通約量”（公約数）という．なるべく大きい通約量を求める問題の解法が互除法である



基準となる最大の長さ

既約分数

$$\frac{b}{a}, \qquad (a,b)=1$$

$a<b$ ⇩

$$b=qa+r, \qquad 0\leq r<a$$

⇩

$$\frac{b}{a}=q+\frac{r}{a}, \qquad 0\leq r<a$$

例題

①
mとnが互いに素な正整数ならば，次式は既約分数

$$\frac{4m+9n}{3m+7n}$$

②
$\frac{8n+7}{5n+6}$が既約分数ではないのはnがどのような整数のときか？

③
$\frac{299}{28}$を掛けても，$\frac{533}{61}$を掛けても正整数になるような，なるべく小さい有理数を求めよ

④
n^2+5と$n+3$のGCDが1でも2でもないのはnがどのような整数のときか？

例題

⑤

$n=1,2,\cdots$ のとき，

$$n^3-5n^2+6n \text{　と　} n^2+5$$

のGCDはnに依存して変わる．このGCDの最大値を求めよ．

⑥

互いに疎な二つの奇数a,bに対して，

$$m=11a+b, \qquad n=3a+b$$

とおくとき，mとnのGCDはaとbに依存して，2,4,8のいずれかになる

⑦

正整数a,bが

$$123456789=(11111+a)(11111-b)$$

を満たしている．このとき，$a-b$は正で，かつ，4の倍数である

今日の提出

- ⑦の具体的なaとbについて考えよ

前回の提出物

n	1	2	3	4	5	6	7	8	9	10
2^n-1	1	3	7	15	31	63	127	255	511	1023
2^n+1	3	5	9	17	33	65	129	257	513	1025

n	11	12	13	14	15	16	17	18	19	20
2^n-1	2047	4095	8191	16383	32767	65535	131071	262143	524287	1048575
2^n+1	2049	4097	8193	16385	32769	65537	131073	262145	524289	1048577

200個までの2^n-1の素数の数12個

200個までの2^n+1の素数の数　5個