

素数とガウス記号に関する問題

問題 1 n を 3 以上の整数, p を素数とするとき,

$$S(n) = \sum_{n < p < n^2} \left[\frac{n^2}{p} \right] < n(n-2)$$

であることを証明せよ.

[解] まず, 記号の意味の確認をしよう. $\left[\frac{n^2}{p} \right]$ の意味するところは $\frac{n^2}{p}$ の整数部分であるが, 見方を変えれば, n^2 以下の自然数で, p の倍数は何個あるかという数ということもできる. それでは $n < p < n^2$ である素数 p の倍数はいくつあるか数えてみよう. $n = 3 \sim 5$ の場合を表 1~3 に示した. $\circ$ の個数が $S(n)$ に相当する ($\bullet$ については後述する). よく見ると, $\circ$ は縦方向に重複していない. つまり一つの列に $\circ$ の数は 0 または

$n = 3$ の場合

	4	5	6	7	8	9
5 の倍数		○				
7 の倍数				○		
3 の倍数			●			●
2 の倍数	●		●		●	

$S(n) = 2$

表 1

$n = 4$ の場合

	5	6	7	8	9	10	11	12	13	14	15	16
5 の倍数	○					○					○	
7 の倍数			○							○		
11 の倍数							○					
13 の倍数									○			
4 の倍数				●				●				●
3 の倍数		●			●			●			●	

$S(n) = 7$

表 2

1 である. これは $n < p$ である任意の二つの素数 p_1, p_2 を考えた場合, その最小公倍数は

$$n^2 < p_1 p_2$$

となり, 範囲を超えてしまうからである. 三つ以上でも同様である. よって, $\circ$ の数は表の (n の) 列の個数を超えることはない. つまり

$$S(n) \leq n^2 - n$$

である. ここから範囲を縮めていくことを目指そう. まず, n 自身の倍数は $n < p < n^2$ である素数 p と等し

		$n = 5$ の場合 $S(n) = 9$																								
		6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25					
7 m			○							○							○									
11 m							○											○								
13 m									○																	
17 m													○													
19 m															○											
23 m																			○							
5 m						●					●					●					●					
4 m			●					●				●				●				●						

表 3

くなることはない．もし等しければ p が合成数になってしまうからである．また n の倍数が p の倍数と等しくなるときは、つまり n, p の公倍数は、最小公倍数が

$$n^2 < np$$

となるので、表の範囲を越してしまう．よって n の倍数は必ず空欄（○がつかないこと）になり、それを●で表した（各表の下から二番目の行）．●は全部で $n - 1$ 個あるので

$$S(n) \leq n^2 - n - (n - 1) = n^2 - 2n + 1$$

となる．だいぶ目標に近づいたが、もう少しだけ範囲を絞らないと証明は達成されない．そこで n より一つ少ない数つまり $n - 1$ の倍数はどうなるか考えてみよう．各表の最下行にそれを示した．今度は○と重なる場合（●で示した）や、 n の倍数と重なる場合（●で示した）があるので単純に引くことはできない．まず、 $n - 1$ の倍数は表の中にいくつ出現するか考えてみよう．

$$n < m(n - 1) < n^2 \quad (1)$$

より

$$1 + \frac{1}{n - 1} = \frac{n}{n - 1} < m < \frac{n^2}{n - 1} = n + 1 + \frac{1}{n - 1}$$

つまり

$$2 \leq m \leq n + 1$$

なのでちょうど n 個である．この中で n の倍数と等しくなるもの（つまり●）について調べてみよう． $n - 1$ と n の最小公倍数は後述の補題 1 より $n(n - 1)$ である．この数は表の中に必ず出現する．この次に大きい公倍数 $2n(n - 1) = 2n^2 - 1$ は ($n \geq 2$ において) n^2 を超えてしまうので、表には現れない．つまり、 $n - 1$ の倍数と、 n の倍数が表の中で重複するのはただの 1 回である．

最後に●について調べよう．●が表の中に現れるということは

$$n < (n - 1)k = jp < n^2$$

を満たす自然数 k, j が存在するということである。 p は素数なので、

$$p \mid n-1 \text{ または } p \mid k$$

$n < p$ だから

$$p \nmid n-1$$

$$\therefore p \mid k$$

よって

$$n < (n-1)ip < n^2$$

を満たす自然数 i があるか調べればよい。(1) と同じ理由により

$$2 \leq ip \leq n+1$$

$p \geq n+1$ なのでこの式を満たすことができるのは $i=1$ のみであり、

$$2 \leq p \leq n+1$$

つまり $p = n+1$ である場合のみである。この場合 $(n-1)(n+1) = n^2 - 1$ が必ず ● となる (表の右から 2 列目)。

最後の最後に ● と ● が重なる場合があるか調べよう。もし重なることがあれば、

$$n(n-1) = (n-1)(n+1)$$

これは $n > 1$ では解を持たないので、重なることはない。

さて、ここまでのことを総合すると、

$n+1$ が素数でない場合

$$S(n) \leq n^2 - 2n + 1 - n + 1 = n^2 - 3n + 2 = n(n-2) + 2 - n \quad (2)$$

$n+1$ が素数の場合

$$S(n) \leq n^2 - 2n + 1 - n + 1 + 1 = n^2 - 3n + 3 = n(n-2) + 3 - n \quad (3)$$

$n=3$ は (2) の場合に相当し、

$$S(n) < n(n-2) \quad (4)$$

を満たす。 $n \geq 4$ の場合は (2),(3) 両方の場合があるが、どちらにしても (4) を満たす。 [証明おわり]

補題 1 自然数 n について、 n と $n+1$ の最小公倍数は $n(n+1)$ である。

[証明] n の倍数を mn 、 $n+1$ の倍数を $k(n+1)$ で表すと (m, k は自然数)、 n と $n+1$ の公倍数は

$$mn = k(n+1)$$

を満たす。当然ながら

$$m > k$$

である。

$$(m-k)n = k$$

であるので k は n の倍数でなければならない．そのなかの最小の $k = n$ について調べると確かに $n(n+1)$ は n と $n+1$ の公倍数であるのでこれが最小である． [証明おわり]

[別解] 数学的帰納法を使ってみよう． $S(n) < n(n-2)$ と仮定して， $S(n+1) < (n+1)(n-1) = n^2 - 1$ が成り立てば証明できたことになる．[解] のように表を使って考えると， n から $n+1$ になった場合，表の一番左の列は消える．そこに $\circ$ がついていた場合 $S(n)$ は一つ以上減るのだが（つまり n が素数だったら $n+1$ になったときに，最上行がなくなるわけだが），素数がどうかはわからないのでここでは問題にしない．表の右には $2n+1$ 列加わることになる．これらの列が全て $\circ$ で埋まっていたとしても，

$$S(n+1) < n^2 - 2n + 2n + 1 = n^2 + 1$$

が言えるが，これではまだ 2 つ多い．まず一番右端の列，つまり $(n+1)^2$ の列は必ず空欄になる． $n(n+1) = n^2 + n$ も空欄である．よって二つは必ず $\circ$ のつかない列で， $S(n+1) < n^2 - 1$ が成り立つ． n^2 と $(n+1)^2$ の間に素数があって，表の行が下に増える場合は問題にしなかった．これは新たに加わった素数による $\circ$ は全て右側の新たに加わった列に $\circ$ があるのでもうすでに数えられているのである． [証明おわり]