EXAMPLES

ANTHONY V. PULIDO

In the following note, we work through theorem 2 of Langlands's essay *A little bit of number theory* for the primes 3 and 5. The theorem claims that two numbers A_p and B_p for p prime are equal. We show that $A_3 = B_3$ and $A_5 = B_5$. Later, we give the results of a computer program that calculates A_p and B_p for any p as a table for the first 100 odd primes.

We state the theorem:

Theorem.

(a) *If* $p \equiv 3 \pmod 4$ *then* $A_p = 0$. *If* $p \equiv 1 \pmod 4$ *write* $p = x^2 + y^2$ *with* (x, y) *congruent to* $(1, 0)$ *or to* $(-1, 2)$ *modulo* 4 *and set* $A_p = 2(x^3 - 3xy^2)$.

(b) *If* $p \equiv 3 \pmod 4$ *set*

$$B_p = \sum\{\alpha^2 + \beta^2 - \gamma^2 - \delta^2\} - \sum\{\alpha^2 + \beta^2 - \gamma^2 - \delta^2\}$$

The first sum is over 4*-tuples such that* $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = p$, $\alpha \equiv 1 \pmod 4$, *and* (β, γ, δ) *is congruent modulo* 4 *to one of* $(0, 1, 1)$, $(2, 3, 3)$, $(0, 3, 3)$, $(2, 1, 1)$. *The second sum is similar but now* (β, γ, δ) *is congruent to one of* $(0, 3, 1)$, $(2, 1, 3)$, $(0, 1, 3)$, $(2, 3, 1)$.

But if $p \equiv 1 \pmod 4$ *set*

$$B_p = \sum\{\alpha^2 + \beta^2 - \gamma^2 - \delta^2\} - \sum\{\alpha^2 + \beta^2 - \gamma^2 - \delta^2\}$$

The two sums are defined similarly. Again $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = p$ *and* $\alpha \equiv 1 \pmod 4$, *but in the first sum* (β, γ, δ) *is congruent modulo* 4 *to one of* $(0, 0, 0)$, $(2, 0, 0)$, $(0, 2, 2)$, $(2, 2, 2)$ *and in the second to one of* $(2, 2, 0)$, $(0, 2, 0)$, $(2, 0, 2)$, $(0, 0, 2)$.

1. $A_3 = B_3$

Let $p = 3$ and

$$A = \sum \left\{\alpha^2 + \beta^2 - \gamma^2 - \delta^2\right\},$$

Date: March 16, 2017.

where this sum is the first one in the definition of B_3. We define the number B similarly. Then, $B_3 = A - B$.

We calculate B_3 first. To determine the ranges of summation of A and B, we list the possible decompositions of 3 as a sum of four squares subject to the constraints of the theorem. It is clear that $\alpha = 1$, and so we obtain the following:

$$\begin{aligned} 3 &= 1^2 + 0^2 + 1^2 + 1^2 && (0,1,1) \\ &= 1^2 + 0^2 + (-1)^2 + (-1)^2 && (0,3,3) \\ &= 1^2 + 0^2 + (-1)^2 + 1^2 && (0,3,1) \\ &= 1^2 + 0^2 + 1^2 + (-1)^2 && (0,1,3) \end{aligned}$$

For each triple (b, g, d) on the right, $(\beta, \gamma, \delta) \equiv (b, g, d) \pmod 4$. We calculate B_3:

$$\begin{aligned} A = &\ 1^2 + 0^2 - 1^2 - 1^2 + \\ &\ 1^2 + 0^2 - (-1)^2 - (-1)^2 \\ = &\ -2. \\ B = &\ 1^2 + 0^2 - (-1)^2 - 1^2 + \\ &\ 1^2 + 0^2 - 1^2 - (-1)^2 \\ = &\ -2. \end{aligned}$$

It follows that $B_3 = A - B = 0$. By part (a), since $3 \equiv 3 \pmod 4$, $A_3 = 0$. $A_3 = B_3 = 0$.

2. $A_5 = B_5$

Since $5 \equiv 1 \pmod 4$, we write $5 = x^2 + y^2 = (-1)^2 + 2^2$. Then,

$$A_5 = 2(x^3 - 3xy^2) = 2((-1)^3 - 3(-1)(2^2)) = 2(-1 + 12) = 22.$$

Using A and B defined in the previous section, we calculate B_5.

$$\begin{aligned} A = &\ 1^2 + 2^2 - 0^2 - 0^2 + && (2,0,0) \\ &\ 1^2 + (-2)^2 - 0^2 - 0^2 \\ = &\ 10 \\ B = &\ 1^2 + 0^2 - 2^2 - 0^2 + && (0,2,0) \\ &\ 1^2 + 0^2 - (-2)^2 - 0^2 + \\ &\ 1^2 + 0^2 - 0^2 - 2^2 + && (0,0,2) \\ &\ 1^2 + 0^2 - 0^2 - (-2)^2 \\ = &\ -3 \cdot 4 = -12. \end{aligned}$$

Finally, $B_5 = A - B = 10 - (-12) = 22$. It follows that $A_5 = B_5$.

3. Program

The Haskell program `lbnt.hs` calculates A_p and B_p for the first 100 odd primes. It can be easily modified to calculate any number of primes, subject of course to the computing power of the hardware on which it is run. Please see the comments in the source code.

The author is a novice programmer, and so the program can likely be greatly optimized. On a mid-2012 Macbook Pro 2.3 GHz Intel Core i7, execution time was about 9 minutes 40 seconds compiled and about 20 minutes interpreted.

The result follows:

nth odd prime	p	$p \pmod 4$	A_p	B_p
1	3	3	0	0
2	5	1	22	22
3	7	3	0	0
4	11	3	0	0
5	13	1	−18	−18
6	17	1	−94	−94
7	19	3	0	0
8	23	3	0	0
9	29	1	−130	−130
10	31	3	0	0
11	37	1	214	214
12	41	1	−230	−230
13	43	3	0	0
14	47	3	0	0
15	53	1	518	518
16	59	3	0	0
17	61	1	830	830
18	67	3	0	0
19	71	3	0	0
20	73	1	1098	1098
21	79	3	0	0
22	83	3	0	0
23	89	1	−1670	−1670
24	97	1	594	594
25	101	1	598	598
26	103	3	0	0
27	107	3	0	0
28	109	1	−1746	−1746

29	113	1	2002	2002
30	127	3	0	0
31	131	3	0	0
32	137	1	−1606	−1606
33	139	3	0	0
34	149	1	−3514	−3514
35	151	3	0	0
36	157	1	286	286
37	163	3	0	0
38	167	3	0	0
39	173	1	−4082	−4082
40	179	3	0	0
41	181	1	3942	3942
42	191	3	0	0
43	193	1	5362	5362
44	197	1	1174	1174
45	199	3	0	0
46	211	3	0	0
47	223	3	0	0
48	227	3	0	0
49	229	1	6390	6390
50	233	1	−598	−598
51	239	3	0	0
52	241	1	−5310	−5310
53	251	3	0	0
54	257	1	−1534	−1534
55	263	3	0	0
56	269	1	3406	3406
57	271	3	0	0
58	277	1	9126	9126
59	281	1	−7430	−7430
60	283	3	0	0
61	293	1	−9418	−9418
62	307	3	0	0
63	311	3	0	0
64	313	1	−6838	−6838
65	317	1	−10274	−10274
66	331	3	0	0
67	337	1	−12366	−12366
68	347	3	0	0
69	349	1	9470	9470

70	353	1	3298	3298
71	359	3	0	0
72	367	3	0	0
73	373	1	−12922	−12922
74	379	3	0	0
75	383	3	0	0
76	389	1	374	374
77	397	1	9614	9614
78	401	1	−2398	−2398
79	409	1	7146	7146
80	419	3	0	0
81	421	1	−10890	−10890
82	431	3	0	0
83	433	1	−4862	−4862
84	439	3	0	0
85	443	3	0	0
86	449	1	16114	16114
87	457	1	16506	16506
88	461	1	2318	2318
89	463	3	0	0
90	467	3	0	0
91	479	3	0	0
92	487	3	0	0
93	491	3	0	0
94	499	3	0	0
95	503	3	0	0
96	509	1	14270	14270
97	521	1	23738	23738
98	523	3	0	0
99	541	1	−5922	−5922
100	547	3	0	0