KNAW 54 1951

1479
1480

MATHEMATICS

THE PRIMES IN $k(\varrho)$

BY

BALTH. VAN DER POL AND PIERRE SPEZIALI

(Communicated at the meeting of December 23, 1950)

In the same way as the complex or Gaussian integers $a + bi$ (a and b rational integers) belong to the field $k(i)$, the integers $\xi = a + b\varrho$ (a and b again rational integers) are said [1]) to belong to the field $k(\varrho)$. Here ϱ is defined as a root of the equation

$$\varrho^2 + \varrho + 1 = 0.$$

The units of $k(\varrho)$ are ± 1, $\pm \varrho$, $\pm \varrho^2$, situated at the corners of a regular hexagon inscribed in the unit circle.

If $\varrho = \frac{1}{2}(-1 + i\sqrt{3}) = e^{\frac{2}{3}i\pi}$, then $\varrho^2 = \frac{1}{2}(-1 - i\sqrt{3}) = e^{\frac{4}{3}i\pi}$

and

$$\varrho + \varrho^2 = -1, \qquad \varrho\varrho^2 = 1.$$

Again we have

$$(\xi - a - b\varrho)\ (\xi - a - b\varrho^2) = 0$$

or

$$\xi^2 - (2a - b)\ \xi + a^2 - ab + b^2 = 0$$

so that ξ is a quadratic integer.

Further it follows from the fundamental relation

$$\varrho^2 + \varrho + 1 = 0,$$

that

$$a + b\varrho = a - b - b\varrho^2,$$

$$a + b\varrho^2 = a - b - b\varrho$$

The integers of $k(\varrho)$ are therefore either of the form $a + b\varrho$ or $a + b\varrho^2$, the one being deducible from the other.

Apart from $1 - \varrho$ with its associates and the rational primes of the form $3n + 2$ with their associates, the primes of $k(\varrho)$ are of the form

$$a + b\varrho$$

---

1) HARDY and WRIGHT, An Introduction to the Theory of Numbers, pp. 177—188 and 220, 221 (Oxford, 1938).

together with their associates, where a and b have to fulfill the relation

(1) $$a^2 - ab + b^2 = p,$$

p being a rational prime of the form

(2) $$p = 3n + 1$$

From (1) and (2) it follows that a and b can not both be even, for then (1) would be even, which is impossible. Again, if a and b are both odd, we can introduce b' defined by $b = a - b'$, where b' is therefore even.

Substitution hereof in (1) yields

$$a^2 - ab' + b'^2$$

which is of the same form as (1) so that we are free to assume b even. We can therefore write

$$b = 2\beta \quad (\beta = \text{integer})$$

and (1) becomes

$$a^2 - ab + b^2 = (a - \tfrac{b}{2})^2 + \tfrac{3}{4}\, b^2 = (a - \beta)^2 + 3\beta^2$$

or calling $a - \beta = c$

$$a^2 - ab + b^2 = c^2 + 3\beta^2$$

Hence we have

(3) $$c^2 + 3\beta^2 = p = 3n + 1$$

It follows from (3) that c cannot be divisible by 3 and thus we are left with the two possibilities $c \equiv 1$ (3) or $c \equiv 2$ (3).

Further in (3) n cannot be odd because this would make $3n + 1$ even.

We can therefore write $n = 2m$ so that (3) becomes

(4) $$c^2 + 3\beta^2 = p = 6m + 1$$

where now m can be odd or even.

Returning to the form $a + b\varrho$, we therefore have

$$a + b\varrho = a + b\left(-\frac{1}{2} + \frac{i\sqrt{3}}{2}\right) = a - \frac{b}{2} + \frac{ib}{2}\sqrt{3} = a - \beta + i\beta\sqrt{3} = c + i\beta\sqrt{3}$$

and hence $c + i\beta\sqrt{3}$ is a prime in $k(\varrho)$, when (4) is fulfilled. E.g. we have

$$1^2 + 3 . 2^2 = 13 = 6 . 2 + 1$$

so that $c = 1$, $\beta = 2$ and $1 + 2i\sqrt{3}$ is a prime in $k(\varrho)$ together with its associates, which are obtained by multiplication by $e^{\frac{k i \pi}{3}}$ $(k = 1, 2, \ldots, 6)$.

We further note that if in the form $a^2 - ab + b^2$ we replace a by $-a$, and b by $-b$ or a by $a - b$ and b by $b - a$, we find the associates of $a + b\varrho$.

The numbers $a + b\varrho$ have been introduced by Eisenstein and Jacobi in their work on cubic reciprocity.

The rational primes of the form $p = 6m + 1$ have already been the subject of several researches. It has been shown that their number is infinite [2]) by considering the expression $3(1 \cdot 2 \cdot 3 \ldots p)^2 + 1$.

Amongst the quadratic forms representing a series of primes of the form $p = 6m + 1$, we note

$$y_1 = 6x^2 + 6x + 31$$

which, for $x = 0, 1, \ldots 28$, yields 29 primes of the form $6m + 1$ comprised between 31 and 4909; replacing x by $x - 29$ we obtain

$$y_2 = 6x^2 - 342x + 4903$$

which yields 58 primes of the form considered. Both forms have been kindly communicated to us by Mr C. COXE (Geneva).

It is the purpose of this note to decompose the primes of the form $6m + 1$ in the form $c^2 + 3\beta^2$ and to represent them in the complex plane $(c, i\beta)$.

Between 1 and 10.000 there are 1229 primes in all, of which 611 are of the form $6m + 1$. Here follows the way in which this decomposition has been effected.

The relation $6m + 1 = c^2 + 3\beta^2$ tells us that:

1) c is not divisible by 3,
2) if c is even then β is odd,
3) if c is odd then β is even.

This means that in the real plane (c, β) all the numbers of the form $6m + 1$, prime or not, are situated on the vertices of hexagons (see Fig. 1).

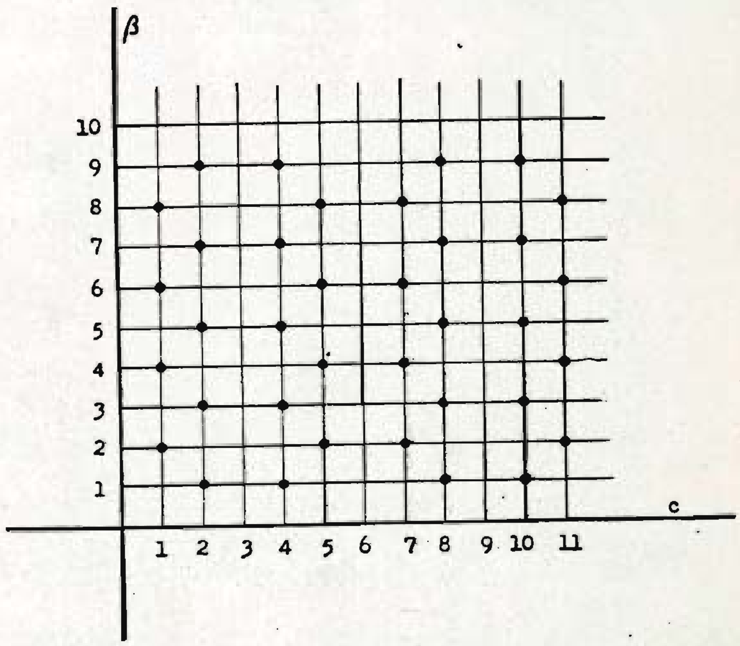


Fig. 1

[2]) E. CAHEN, Eléments de la Théorie des Nombres, p. 319 (Paris, 1900).

Instead of attempting the decomposition directly, which would mean more and more trials, the following course was followed.

After a list of primes of the form $6m + 1$ was prepared, the following additions were made:

$$2^2 + 3.1^2,\ 4^2 + 3.1^2,\ 8^2 + 3.1^2 \ldots$$

$$1^2 + 3.2^2,\ 5^2 + 3.2^2,\ 7^2 + 3.2^2 \ldots \text{ etc.}$$

and it was verified whether such a sum gave a prime of the required form. Of course also columns instead of lines could have been followed.

Below we give a table of the decompositions of the primes of the form $p = 6m + 1$ into the form $c^2 + 3\beta^2$.

The first column gives the primes p and the second the numbers c and β.

The representation of the primes $c + i\beta\sqrt{3}$ of the field $k(\varrho)$ in the complex plane is most naturally effected by first covering the plane with a net of adjacent regular hexagons. The distance of the centres of two horizontally adjacent hexagons is taken as the unit distance.

Then the shortest distance between two centres situated on a vertical becomes $\sqrt{3}$.

E.g. the point A in Fig. 2 represents the complex prime $4 + 1i\sqrt{3}$.

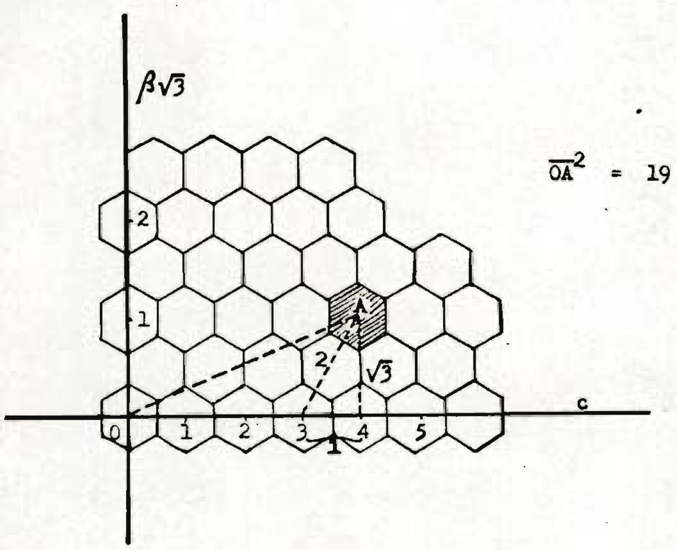
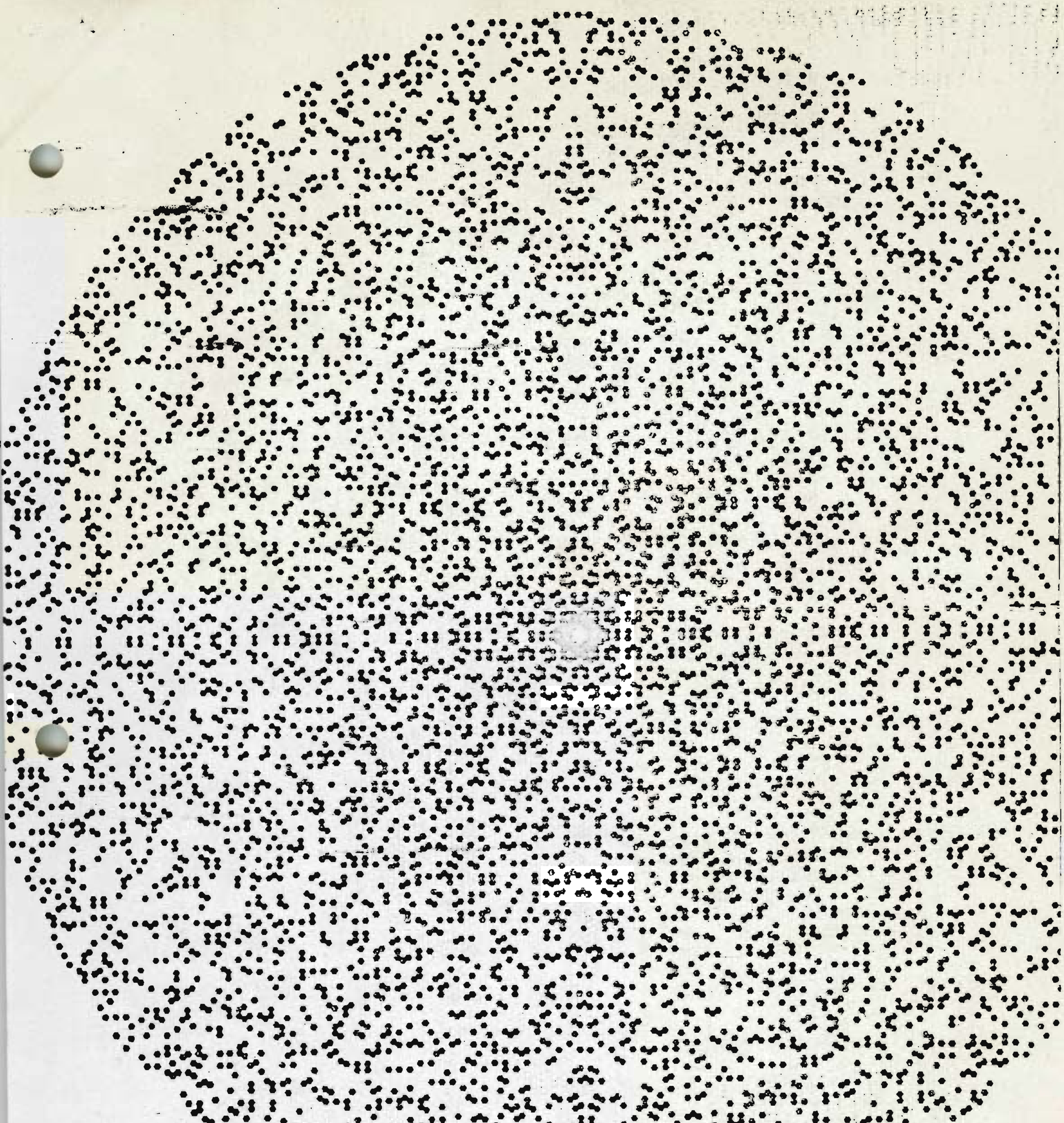


Fig. 2

Its norm $N(4 + 1i\sqrt{3}) = (4 + i\sqrt{3})\ (4 - i\sqrt{3}) = 19$ is a rational prime of the form $6m + 1$. The hexagon having A as its centre has been shaded together with its associates $e^{\frac{ki\pi}{3}}\ (4 + i\sqrt{3})$, $k = 1, 2, \ldots 6$.

These associates are therefore simply found by turning over angles of 60°, 120°, 180°, ... etc. In this way the large diagram of Plate I was



constructed which clearly shows the symmetries around the angles 0°, 60°, 120°, ...

The centre of this Plate is illustrated separately in Fig. 3.

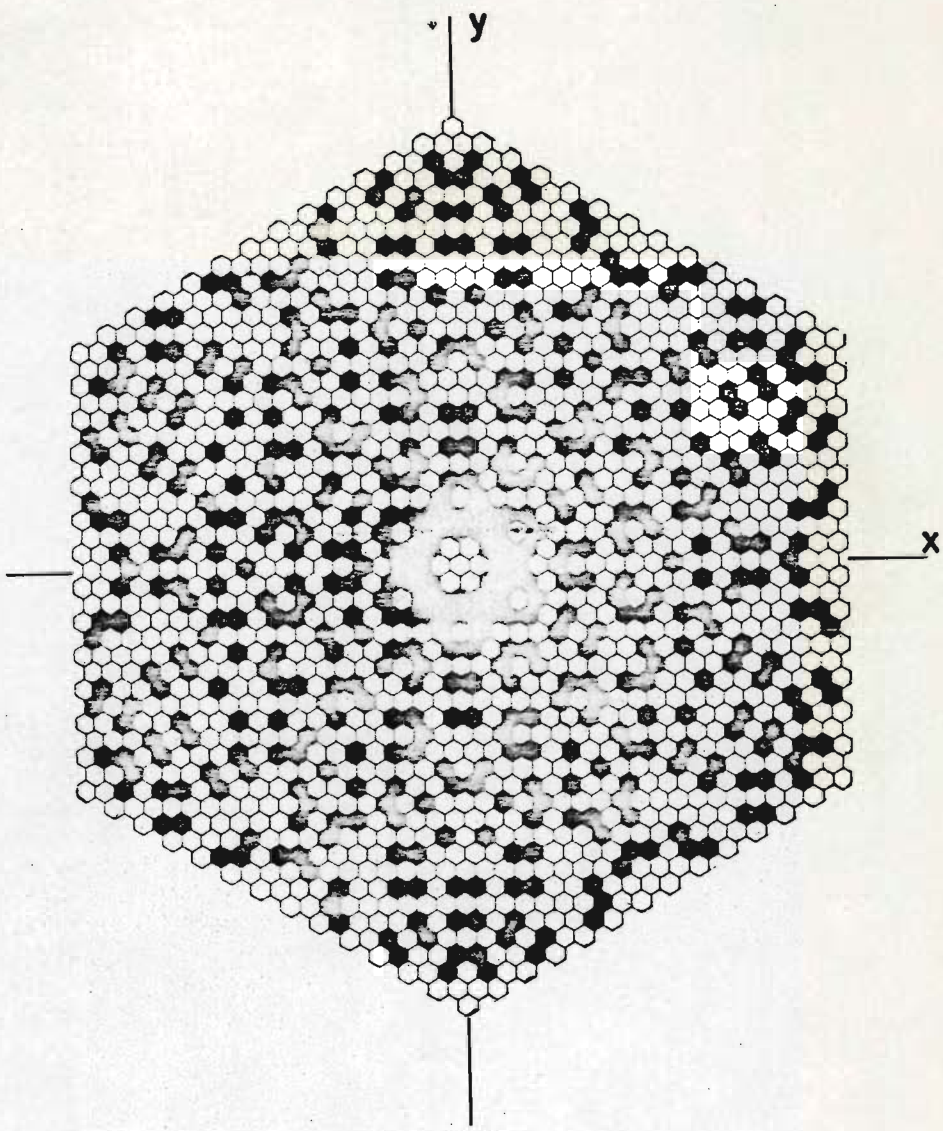


Fig 3.

A similar diagram of the Gaussian primes (of the field $k(i)$) was published previously [3].

Genève, Dec. 1950.

[3]) BALTH. VAN DER POL, Verslagen van de Maatschappij Diligentia, ('s-Gravenhage, 1946).

A decomposition of the primes
Type 3. Ref ~~UNAW~~
54 14 51

1479 1480

TABLE

of the decomposition of the primes below 10.000 of the form $p = 6m + 1$ into the form $c^2 + 3\beta^2$

p	c, β	p	c, β	p	c, β	p	c, β	p	c, β	p	c, β
7	2,1	571	8,13	1231	34,5	1951	38,13	2713	19,28	3517	7,34
13	1,2	577	23,4	1237	35,2	1987	20,23	2719	14,29	3529	59,4
19	4,1	601	13.12	1249	7,20	1993	35.16	2731	52,3	3541	29,30
31	2,3	607	10,13	1279	14,19	1999	26,21	2749	7,30	3547	32,29
37	5,2	613	5,14	1291	28,13	2011	44,5	2767	38,21	3559	26,31
43	4,3	619	16,11	1297	23,16	2017	17,24	2791	46,15	3571	52,17
61	7,2	631	22,7	1303	34,7	2029	1,26	2797	47,14	3583	50,19
67	8,1	643	20,9	1321	11,20	2053	5,26	2803	44,17	3607	58,9
73	5,4	661	19,10	1327	2,21	2083	44,7	2833	49,12	3613	55,14
79	2,5	673	25,4	1381	37,2	2089	19,24	2851	52,7	3631	38,27
97	7,4	691	4,15	1399	34,9	2113	41,12	2857	53,4	3637	13,34
103	10,1	709	11,14	1423	10,21	2131	16.25	2887	2,31	3643	56,13
109	1,6	727	22,9	1429	29,14	2137	37,16	2917	53,6	3673	59,8
127	10,3	733	25,6	1447	38,1	2143	46,3	2953	35,24	3691	4,35
139	8,5	739	8,15	1453	1,22	2161	31,20	2971	28,27	3697	25,32
151	2,7	751	26,5	1459	28,15	2179	44.9	3001	53,8	3709	41,26
157	7,6	757	13,14	1471	38,3	2203	4,27	3019	44,19	3727	58,11
163	4,7	769	1.16	1483	20,19	2221	47,2	3037	55,2	3733	61,2
181	13,2	787	28,1	1489	17,20	2239	34,19	3049.	43,20	3739	8,35
193	1.8	811	28,3	1531	32,13	2251	8,27	3061	19,30	3769	61,4
199	14,1	823	26,7	1543	26,17	2269	41.14	3067	52,11	3793	55,16
211	8,7	829	23,10	1559	31.14	2281	43,12	3079	14,31	3823	50,21
223	14,3	853	29,2	1567	22,19	2287	10,27	3109	53,10	3847	62,1
229	11.6	859	28,5	1579	16,21	2293	29,22	3121	7,32	3853	49,22
241	7,8	877	17,14	1597	25,18	2311	38.17	3163	56,3	3877	43,26
271	14,5	883	4,17	1609	29,16	2341	37,18	3169	49,16	3889	1,36
277	13,6	907	20,13	1621	13,22	2347	32,21	3181	47,18	3907	32,31
283	16,3	919	26,9	1627	40,3	2371	28,23	3187	40,23	3919	62,5
307	8,9	937	13,16	1657	35,12	2377	5,28	3217	55,8	3931	16,35
313	11,8	967	10,17	1663	34,13	2383	14,27	3229	23,30	3943	26,33
331	16,5	991	22,13	1669	37,10	2389	19.26	3253	35,26	3967	38,29
337	17,4	997	5,18	1693	41,2	2437	43,14	3259	44,21	4003	56,17
349	7,10	1009	31,4	1699	32,15	2467	40,17	3271	2,33	4021	61,10
367	2,11	1021	7,18	1723	20,21	2473	11,28	3301	43,22	4027	52,21
373	19,2	1033	29,8	1741	17,22	2503	50.1	3307	28,29	4051	28,33
379	4,11	1039	26,11	1747	40,7	2521	13,28	3313	31,28	4057	13,36
397	17,6	1051	32,3	1753	5,24	2539	4.29	3319	38.25	4093	25,34
409	19,4	1063	14,17	1759	26,19	2551	26,25	3331	8,33	4099	64,1
421	11,10	1069	31,6	1777	7,24	2557	23,26	3343	34,27	4111	2,37
433	1,12	1087	2,19	1783	14,23	2593	49,8	3361	17,32	4129	49,24
439	14,9	1093	11,18	1789	41,6	2617	43,16	3373	49.18	4153	61,12
457	5,12	1117	23,14	1801	37.12	2647	50,7	3391	58,3	4159	22,35
463	10,11	1123	16.17	1831	34,15	2659	28,25	3433	19,32	4177	17,36
487	22,1	1129	19,16	1861	43,2	2671	22,27	3457	55,12	4201	43,28
499	16,9	1153	31,8	1867	28,19	2677	35.22	3463	14,33	4219	56,19
523	4,13	1171	32,7	1873	41,8	2683	40,19	3469	1,34	4231	58,17
541	23,2	1201	1,20	1879	2,25	2689	31,24	3499	56,11	4243	64,7
547	20,7	1213	25,14	1933	31.18	2707	52,1	3511	58,7	4261	53,22

he form $p = 6m + 1$ into

p	c, β	p	c, β
2713	19,28	3517	7,34
2719	14,29	3529	59,4
2731	52,3	3541	29,30
2749	7,30	3547	32,29
2767	38,21	3559	26,31
2791	46,15	3571	52,17
2797	47,14	3583	50,19
2803	44,17	3607	58,9
2833	49,12	3613	55,14
2851	52,7	3631	38,27
2857	53,4	3637	13,34
2887	2,31	3643	56,13
2917	53,6	3673	59,8
2953	35,24	3691	4,35
2971	28,27	3697	25,32
3001	53,8	3709	41,26
3019	44,19	3727	58,11
3037	55,2	3733	61,2
3049	43,20	3739	8,35
3061	19,30	3769	61,4
3067	,11	3793	55,16
3079	14,31	3823	50,21
3109	53,10	3847	62,1
3121	7,32	3853	49,22
3163	56,3	3877	43,26
3169	49,16	3889	1,36
181	47,18	3907	32,31
187	40,23	3919	62,5
217	55,8	3931	16,35
229	23,30	3943	26,33
253	35,26	3967	38,29
259	44,21	4003	56,17
271	2,33	4021	61,10
301	43,22	4027	52,21
307	28,29	4051	28,33
313	31,28	4057	13,36
19	38,25	4093	25,34
31	8,33	4099	64,1
43	34,27	4111	2,37
61	17,32	4129	49,24
73	49,18	4153	61,12
91	58,3	4159	22,35
33	19,32	4177	17,36
57	55,12	4201	43,28
63	14,33	4219	56,19
[illegible]	1,34	4231	58,17
49	56,11	4243	64,7
11	58,7	4261	53,22

p	c, β	p	c, β	p	c, β	p	c, β	p	c, β	p	c, β
4273	65,4	5227	52,29	6211	68,23	7177	37,44	8191	46.45	9091	4,55
4297	35,32	5233	71,8	6217	67,24	7207	2,49	8209	49,44	9103	26,53
4327	38,31	5281	47,32	6229	77,10	7213	79,18	8221	89,10	9109	19,54
4339	64,9	5323	56.27	6247	58,31	7219	4,49	8233	11,52	9127	50,47
4357	5,38	5347	28,39	6271	14,45	7237	85,2	8263	86,17	9133	95,6
4363	16,37	5407	70,13	6277	53,34	7243	56,37	8269	79,26	9151	74,35
4423	34,33	5413	11,42	6301	73,18	7297	65,32	8287	22,51	9157	53,46
4441	37,32	5419	64,21	6337	23,44	7309	31,46	8293	91,2	9181	41,50
4447	58,19	5431	62,23	6343	74,17	7321	83,12	8311	82,23	9187	68,39
4483	40,31	5437	73,6	6361	77,12	7333	85,6	8317	55,42	9199	94,11
4507	20,37	5443	20,41	6367	62,29	7351	74,25	8329	91,4	9241	83,28
4513	25,36	5449	61,24	6373	5,46	7369	59,36	8353	89,12	9277	23,54
4519	62,15	5479	74,1	6379	52,35	7393	71,28	8377	67,36	9283	80,31
4549	43,30	5503	74,3	6397	7,46	7411	28,47	8389	91,6	9319	46,49
4561	47,28	5521	73,8	6421	61,30	7417	85,8	8419	88,15	9337	35,52
4567	2,39	5527	22,41	6427	80,3	7459	16,49	8431	2,53	9343	94,13
4591	22,37	5557	35,38	6451	76,15	7477	83,14	8443	4,53	9349	43,50
4597	67,6	5563	4,43	6469	11,46	7489	41,44	8461	31,50	9391	62,43
4603	64,13	5569	41,36	6481	41,40	7507	68,31	8467	92,1	9397	77,34
4621	17,38	5581	17.42	6529	73,20	7537	25,48	8521	61,40	9403	40,51
4639	46,29	5623	74,7	6547	80,7	7459	7,50	8527	10,53	9421	97,2
4651	68,3	5641	29.40	6553	59,32	7561	67,32	8539	92,5	9433	5,56
4657	65,12	5647	10,43	6571	32,43	7573	35,46	8563	44,47	9439	58,45
4663	10,39	5653	19,42	6577	65,28	7591	82,17	8581	91,10	9463	70,39
4723	56,23	5659	56,29	6607	50,37	7603	20,49	8599	82,25	9511	94,15
4729	29,36	5683	64,23	6619	64,29	7621	11,50	8623	14,53	9547	92,19
4759	14,39	5689	67,20	6637	17,46	7639	86,9	8629	77,30	9601	97,8
4783	26,37	5701	37.38	6661	37,42	7669	13,50	8641	23,52	9613	95,14
4789	67,10	5737	43,36	6673	79,12	7681	73,28	8647	38,49	9619	88,25
4801	1,40	5743	14,43	6679	46,39	7687	22,49	8677	85,22	9631	98,3
4813	65,14	5749	61,26	6691	8,47	7699	56,39	8689	89,16	9643	64,43
4831	34,35	5779	76,1	6703	34,43	7717	37.46	8707	92,9	9649	89,24
4861	23,38	5791	46,35	6709	19,46	7723	80,21	8713	91,12	9661	73,38
4903	70,1	5821	23,42	6733	49,38	7741	71,30	8719	86,21	9679	98,5
4909	47,30	5827	28,41	6763	80,11	7753	29.48	8731	68,37	9697	17,56
4933	59,22	5839	74,11	6781	73,22	7759	86,11	8737	25,52	9721	53,48
4951	58,23	5851	76,5	6793	61,32	7789	17,50	8761	43,48	9733	91,22
4957	25,38	5857	7,44	6823	14,47	7867	8,51	8779	52,45	9739	44,51
4969	13,40	5869	49,34	6829	79,14	7873	31,48	8803	40,49	9769	19,56
4987	68,11	5881	53.32	6841	67,28	7879	26.49	8821	67,38	9781	67,42
4993	65,16	5923	76,7	6871	82,7	7927	58,39	8839	94,1	9787	92,21
4999	46,31	5953	65,24	6883	16,47	7933	89,2	8863	94,3	9811	8,57
5011	56,25	6007	38,39	6907	80,13	7951	62,37	8887	62,41	9817	77,36
5023	50,29	6037	77,6	6949	59,34	7963	76,27	8893	89,18	9829	59,46
5059	4,41	6043	44,37	6961	7,48	7993	85,16	8923	80,29	9859	28,55
5077	67,14	6067	32,41	6967	82,9	8011	44,45	8929	71,36	9871	38,53
5101	49,30	6073	61.28	6991	38,43	8017	47,44	8941	79,30	9883	76,37
5107	8,41	6079	2,45	6997	83,6	8053	61,38	8971	92,13	9901	49,50
5113	35,36	6091	4,45	7027	20.47	8059	16,51	9001	77,32	9907	52,49
5119	38,35	6121	77,8	7039	58,35	8089	83,20	9007	70,37	9931	88,27
5167	62,21	6133	29,42	7057	73,24	8101	53,42	9013	61,42	9949	89,26
5179	64,19	6151	74,15	7069	71,26	8161	7,52	9043	76,33	9967	98,11
5197	65,18	6163	40,39	7129	77,20	8167	70,33	9049	91,16	9973	35,54
5209	59,24	6199	34,41	7159	46,41	8179	56,41	9067	88,21		