SITZUNGSBERICHTE

DER

KÖNIGLICH PREUSSISCHEN

AKADEMIE DER WISSENSCHAFTEN

JAHRGANG 1913

ZWEITER HALBBAND. JULI BIS DECEMBER

STÜCK XXXIII—LIII MIT EINER TAFEL,
DEM VERZEICHNISS DER EINGEGANGENEN DRUCKSCHRIFTEN, NAMEN- UND SACHREGISTER

BERLIN 1913

VERLAG DER KÖNIGLICHEN AKADEMIE DER WISSENSCHAFTEN

IN COMMISSION BEI GEORG REIMER

Über die Teilbarkeit von $2^p - 2$ durch das Quadrat der Primzahl $p = 1093$.

Von WALDEMAR MEISSNER.

(Vorgelegt von Hrn. FROBENIUS.)

Wenn der FERMATschen Gleichung

$$x^p + y^p + z^p = 0 \tag{1.}$$

drei ganze Zahlen genügen, von denen keine durch die ungerade Primzahl p teilbar ist, so muß, wie Hr. WIEFERICH (*CRELLES Journ. Bd. 136*) gezeigt hat,

$$2^{p-1} \equiv 1 \pmod{p^2} \tag{2.}$$

sein, und wie Hr. MIRIMANOFF (*ebenda Bd. 139*) bewiesen hat, auch

$$3^{p-1} \equiv 1 \pmod{p^2} \tag{3.}$$

sein. Die wahre Quelle dieser Ergebnisse hat Hr. FURTWÄNGLER aufgedeckt, indem er (*Wiener Sitzungsber. Bd. 121*) aus dem EISENSTEINschen Reziprozitätsgesetze den Satz abgeleitet hat:

Sind x, y, z drei ganze Zahlen ohne gemeinsamen Teiler, zwischen denen die FERMATsche Gleichung besteht, so ist

$$r^{p-1} \equiv 1 \pmod{p^2} \tag{4.}$$

für jeden Faktor r von x, falls x nicht durch p teilbar ist, und für jeden Faktor r von $x^2 - y^2$, falls $x^2 - y^2$ nicht durch p teilbar ist.

Gehört $r \pmod p$ zum Exponenten t, so ist

$$r^{p-1} - 1 \equiv \frac{p-1}{t}(r^t - 1) \pmod{p^2}, \tag{5.}$$

und daher ist die Kongruenz

$$r^t \equiv 1 \pmod{p^2} \tag{6.}$$

mit der Kongruenz (4.) gleichbedeutend.

ABEL hatte (*CRELLES Journ. Bd. 3, S. 212*) die Frage aufgeworfen, ob überhaupt, wenn p eine Primzahl ist, und r zwischen 1 und p liegt,

$r^{p-1}-1$ durch p^2 teilbar sein kann. JACOBI hat (*ebenda S. 301*) mehrere Fälle dieser Art angegeben, z. B. die Kongruenz

$$3^5 \equiv 1 \pmod{11^2}. \tag{7.}$$

Für die Basis $r = 2$ war es aber bisher nicht gelungen, eine entsprechende Primzahl p zu finden trotz des lebhaften Interesses, das gerade der WIEFERICHsche Satz für diese Frage erweckt hat.

Hr. CUNNINGHAM hat (*Quart. Journ. of Math. vol. 37, p. 122*) für alle Primzahlen und Primzahlpotenzen $p^k < 10000$ die Exponenten t bestimmt, zu denen die Zahl 2 (mod p^k) gehört. Ich selbst habe für alle Primzahlen $p < 2000$ die kleinsten positiven Reste λ von

$$\frac{2^t - 1}{p} \pmod{p}$$

berechnet, und zwar die für $p < 1000$ schon im Jahre 1910.

Hr. GRAWE in Kiew hat vor kurzem in russischer Sprache einen elementaren Abriß der Zahlentheorie herausgegeben. In einer der angehängten Tabellen gibt er für alle Primzahlen $p < 1000$ die Reste[1] von

$$\frac{2^{p-1} - 1}{p} \equiv W(p) \pmod{p}.$$

Wie er S. 315 sagt, glaubt er beweisen zu können, daß die WIEFERICHsche Kongruenz (2.) überhaupt nicht möglich ist. Hätte er seine Tabelle nur noch auf das nächste Hundert ausgedehnt, so hätte er gefunden, daß die Primzahl

$$p = 1093 \tag{8.}$$

der Kongruenz (2.) genügt. Sie ist die einzige Primzahl dieser Art unter 2000.

Die Zahl 2 gehört (mod p) zum Exponenten

$$t = \frac{1}{3}(p-1) = 364 = 4 \cdot 7 \cdot 13. \tag{9.}$$

Da aber

$$p = \frac{3^7 - 1}{3 - 1}, \qquad 3^7 = 1 + 2p \tag{10.}$$

ist, so kann für p das Kriterium von MIRIMANOFF herangezogen werden.

Damit sich jeder mühelos von der Richtigkeit der Behauptung überzeugen kann, teile ich eine Verifikation der von mir entdeckten Kongruenz

$$2^{364} \equiv 1 \pmod{1093^2} \tag{11.}$$

[1] In der Tabelle fehlt $p = 193$. Die richtigen Werte sind für

$p =$	37	193	797	863	881
$W(p) =$	1	104	336	204	293.

mit, die, auf Kunstgriffen des Hrn. CUNNINGHAM beruhend, mir von anderer Seite angegeben worden ist. Genauer ist übrigens

$$(12.) \qquad 2^{364} \equiv 1 - 202\,p^2 \pmod{p^3}.$$

Setzt man

$$(13.) \qquad \mu = 33 + 2i,$$

so ist

$$p = 33^2 + 2^2 = \mu(\mu - 4i) \equiv -4i\mu,$$

nämlich (mod μ^2), wie hier stets zu ergänzen ist. Nun ist

$$2^5 = (\mu - 2i) - 1, \quad 2^{15} \equiv -(2i+1)^3 + 3(2i+1)^2\mu = 11 + 2i + 3(-3 + 4i)\mu,$$

$$3 \cdot 2^{15} \equiv 33 + 6i + (-27 + 36i)\mu \equiv 4i + 2(-13 + 18i)\mu,$$

oder weil $-13 + 18i \equiv 20(1+i) \pmod{\mu}$ ist,

$$3 \cdot 2^{13} \equiv i + 10(1+i)\mu.$$

Genauer ist

$$(14.) \qquad 3 \cdot 2^{13} = i + 10(1+i)\mu + (22 - 3i)\mu^2.$$

Erhebt man jene Kongruenz auf die 14. Potenz, so erhält man

$$3^{14} \cdot 2^{182} \equiv i^{14} + 14i^{13}\,10(1+i)\mu = -1 + 140i(1+i)\mu.$$

Nun ist

$$140 = 4(\mu - 2i) + 8 \equiv 8(1-i) \pmod{\mu}, \qquad p \equiv -4i\mu \pmod{\mu^2},$$

$$3^7 = 1 + 2p, \qquad 3^{14} \equiv 1 + 4p \pmod{p^2},$$

und mithin

$$3^{14} \cdot 2^{182} \equiv -1 + 16i\mu \equiv -1 - 4p \equiv -3^{14},$$

also

$$(15.) \qquad 2^{182} \equiv -1, \qquad 2^{364} \equiv 1 \pmod{p^2}.$$

Aus (14.) ergibt sich genauer

$$(16.) \qquad 2^{182} \equiv -1 + (7-i)\mu^2 \equiv -1 + 101\,p^2 \pmod{\mu^3}.$$

Will man die komplexen Größen vermeiden, so entwickle man in ähnlicher Art die Kongruenz

$$(17.) \qquad 3^2 2^{26} \equiv -1 + \frac{1}{2}\,155p \pmod{p^2}$$

und erhebe sie auf die siebente Potenz.

Zum Schluß gebe ich die Tabelle für die kleinsten positiven Reste von

$$\frac{2^t - 1}{p} \equiv \lambda \pmod{p}$$

für alle Primzahlen $p < 2000$, und nach dem Vorgange des Hrn. CUNNINGHAM die (von mir selbständig berechneten) Werte von

$$\tau = \frac{p-1}{t},$$

so daß nach (5.)

$$W \equiv \frac{2^{p-1}-1}{p} \equiv \tau\lambda$$

ist. Jeder Wert von λ ist auf zwei verschiedenen, voneinander unabhängigen Wegen berechnet.

A1917 (\tau), A2323 (\lambda)

p	τ	λ	p	τ	λ	p	τ	λ	p	τ	λ
3	1	1	181	1	148	421	1	353	673	14	617
5	1	3	91	2	25	31	10	20	77	1	324
7	2	1	93	2	52	33	6	105	83	31	677
11	1	5	97	1	175	39	6	226	91	3	280
13	1	3	99	2	167	43	1	141	701	1	315
17	2	15	211	1	109	49	2	347	09	1	440
19	1	3	23	6	143	57	6	271	19	2	696
23	2	20	27	1	201	61	1	417	27	6	573
29	1	1	29	3	99	63	2	75	33	3	169
31	6	1	33	8	30	67	1	122	39	3	259
37	1	1	39	2	13	79	2	126	43	2	20
41	2	32	41	10	207	87	2	286	51	2	666
43	3	37	51	5	200	91	1	35	57	1	62
47	2	22	57	16	255	99	3	243	61	2	291
53	1	36	63	2	64	503	2	280	69	2	612
59	1	8	69	1	260	09	1	316	73	1	118
61	1	36	71	2	190	21	2	321	87	1	304
67	1	10	77	3	208	23	1	406	97	1	336
71	2	1	81	4	159	41	1	191	809	2	116
73	8	7	83	3	208	47	1	255	11	3	481
79	2	49	93	1	78	57	1	226	21	1	723
83	1	48	307	3	98	63	1	146	23	2	23
89	8	23	11	2	243	69	2	9	27	1	154
97	2	77	13	2	60	71	5	226	29	1	625
101	1	92	17	1	175	77	4	113	39	2	146
03	2	81	31	11	133	87	1	303	53	1	642
07	1	13	37	16	157	93	4	271	57	2	88
09	3	95	47	1	149	99	2	74	59	1	277
13	4	49	49	1	325	601	24	539	63	2	102
27	18	1	53	4	304	07	2	162	77	1	384
31	1	17	59	2	29	13	1	29	81	16	624
37	2	95	67	2	353	17	4	567	83	1	303
39	1	30	73	1	204	19	1	554	87	2	847
49	1	96	79	1	2	31	14	263	907	1	898
51	10	66	83	2	98	41	10	553	11	10	909
57	3	132	89	1	134	43	3	249	19	6	205
63	1	67	97	9	308	47	2	25	29	2	522
67	2	107	401	2	370	53	1	399	37	8	191
73	1	3	09	2	78	59	1	166	41	1	291
79	1	50	19	1	318	61	1	471	47	1	892

p	τ	λ	p	τ	λ	p	τ	λ	p	τ	λ
953	14	559	1231	2	652	1531	1	319	1831	6	1604
67	2	896	37	1	225	43	2	1356	47	2	1381
71	5	447	49	8	824	49	1	635	61	1	61
77	2	99	59	1	876	53	8	202	67	1	499
83	2	195	77	1	384	59	2	995	71	2	738
91	2	584	79	2	908	67	2	1424	73	2	1366
97	3	245	83	1	666	71	1	379	77	1	1142
1009	2	296	89	8	252	79	3	1166	79	2	1624
13	11	453	91	1	65	83	2	469	89	4	1675
19	1	724	97	2	606	97	3	183	1901	1	1722
21	3	932	1301	1	1012	1601	4	1122	07	1	1510
31	2	318	03	2	673	07	2	740	13	8	1006
33	4	642	07	1	784	09	8	947	31	1	1220
39	2	872	19	2	768	13	31	666	33	3	568
49	4	399	21	22	501	19	1	992	49	1	497
51	3	838	27	6	174	21	1	1123	51	2	893
61	1	362	61	2	990	27	3	1437	73	1	384
63	2	297	67	2	829	37	1	29	79	1	606
69	3	417	73	1	190	57	18	743	87	1	1304
87	2	975	81	1	456	63	2	1046	93	2	561
91	1	319	99	6	1030	67	1	1231	97	1	337
93	3	0	1409	2	1110	69	1	968	99	6	1297
97	4	961	23	6	287	93	1	1327			
1103	38	314	27	1	10	97	2	158			
09	1	101	29	17	439	99	3	851			
17	1	319	33	8	1156	1709	7	476			
23	1	1005	39	2	890	21	8	1471			
29	2	560	47	2	933	23	3	1658			
51	2	503	51	1	1437	33	1	8			
53	4	45	53	1	691	41	1	342			
63	7	939	59	3	986	47	1	320			
71	1	298	71	6	185	53	12	730			
81	5	85	81	4	856	59	2	1267			
87	1	345	83	1	1368	77	24	1352			
93	4	1108	87	2	1356	83	2	1466			
1201	4	869	89	2	1058	87	1	1474			
13	1	215	93	1	520	89	3	219			
17	8	723	99	1	204	1801	72	621			
23	2	848	1511	2	969	11	5	63			
29	1	546	23	1	810	23	2	1410			