Folglich ist für $|D| \geqslant 34$ die Ungleichung (2) erfüllt, ebenso für $|D| = 33$, weil 3 Diskriminantenteiler, also $h \leqslant 9$ ist.

Für mögliche Werte D mit $23 \leqslant |D| \leqslant 30$ ist $G = 6$ und daher $h \leqslant 9$. Mithin ist (2) erfüllt für $|D| = 30$ und $|D| = 29$. In $k(\sqrt{-26})$ hat das Primideal $\mathfrak{p} = (2, \sqrt{-26})$ die Ordnung 2, das Primideal $\mathfrak{q} = (3, 1+\sqrt{-26})$ die Ordnung 3. Folglich muß h ein Vielfaches von 6 sein. Wegen $h \leqslant 9$ ist $h = 6$ und (2) erfüllt.

Für mögliche Werte von D mit $16 \leqslant |D| \leqslant 22$ ist $G = 5$, also

$$h \leqslant \sum_{n=1}^{5} F(n) = 5 + \left(\frac{4D}{3}\right) + \left(\frac{4D}{5}\right) \leqslant 7 .$$

Mithin ist (2) erfüllt für $|D| = 22$. Für $|D| = 21$ ist 3 Diskriminantenteiler, also $h \leqslant 6 < \frac{1}{3}|D|$. Für $|D| = 17$ ist $\left(\frac{-4 \cdot 17}{5}\right) = -1$, folglich $h \leqslant 5 < \frac{1}{3}|D|$.

Für mögliche Werte D mit $10 \leqslant |D| \leqslant 15$ ist $G = 4$, also

$$h \leqslant 4 + \left(\frac{4D}{3}\right) \leqslant 5 .$$

In $k(\sqrt{-14})$ hat das Primideal $\mathfrak{q} = (3, 5+2\sqrt{-14})$ die Ordnung 4. Da sie ein Teiler von h sein muß, ist $h = 4$ und (2) für $|D| = 14$ erfüllt. Für $|D| = 13$ und $|D| = 10$ ist $\left(\frac{-4|D|}{3}\right) = -1$, also ebenso $h \leqslant 3 < \frac{1}{3}|D|$.

Da für $D = -6$ und $D = -5$ für ganzrationalzahlige x und y die Gleichung $x^2 - Dy^2 = 2$ keine Lösung hat, ist in diesen beiden Körpern der Primidealteiler von 2 Nebenideal und mithin (siehe oben !) ist für diese beiden Körper $h = 2$. Folglich ist (2) nicht erfüllt für $|D| = 6, 5, 2$ und 1. Damit ist der Beweis auch für negative D erbracht.

Literaturverzeichnis

[1] N. C. Ankeny, E. Artin and S. Chowla, *The class-number of real quadratic number fields*, Ann. Math. 56 (1952), S. 479-493.

[2] N. C. Ankeny and S. Chowla, *A note on the class number of real quadratic fields*, Acta Arith. 6 (1960), S. 145-147.

[3] H. Hasse, *Vorlesungen über Zahlentheorie*, Berlin, Göttingen, Heidelberg 1950.

[4] E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Leipzig 1923.

[5] K. Schaffstein, *Tafel der Klassenzahlen der reellen quadratischen Zahlkörper mit Primzahldiskriminante unter 12000 und zwischen 100000-101000 und 1000000-1001000*, Math. Ann. 98 (1927/28), S. 745-748.

Reçu par la Rédaction le 18. 4. 1962

ACTA ARITHMETICA
VIII (1963)

К вопросу о простых иррегулярных числах

И. Ш. Славутский (Ленинград)

1. Простое нечетное число p называется *иррегулярным*, если p делит числитель хотя бы одного из чисел Бернулли, $B_2, B_4, \ldots, B_{p-3}$ и *регулярным* в противном случае. Здесь числа Бернулли подчинены рекуррентному символическому соотношению $(B+1)^k = B^k$, $k = 2, 3, \ldots, B_0 = 1$. Общеизвестна связь этого понятия с теорией алгебраических чисел, а также с диофантовым анализом (см. [1], [2] и другие). В частности, целый ряд фактов теории кругового поля $R(e^{2\pi i/p})$ существенным образом зависит от того, является ли простое число p регулярным или нет.

Наличие бесконечного количества простых иррегулярных чисел вида $p \equiv 3 \pmod 4$ впервые доказано Иенсеном ([3]) (1). Вопрос о количестве простых иррегулярных чисел вида $p \equiv 1 \pmod 4$ и о количестве регулярных простых чисел остается открытым, хотя далеко продвинутые вычисления на электронных машинах дают повод предполагать, что и тех и других бесконечно много ([7]).

2. Результат Иенсена дополняет следующая

Теорема. *Существует бесконечно много простых иррегулярных чисел вида* $p \equiv 2 \pmod 3$.

Действительно, пусть простых иррегулярных чисел вида $p \equiv 2 \pmod 3$ конечное число: $p_1, \ldots, p_r$. В силу теоремы Дирихле (о простых числах в арифметической прогрессии) можно выбрать целое число g так, чтобы $Q = 3g\prod_{i=1}^{r}(p_i - 1) + 1$ оказалось простым числом. Рассмотрим число Бернулли с номером $T = 4Q$.

Знаменатель B_T равен $30 = 2 \cdot 3 \cdot 5$, как это следует из теоремы Штаудта. Действительно, $2Q + 1 = 3 \cdot 2g\prod_i (p_i - 1) + 3$ и $4Q + 1 = 12g\prod_i (p_i - 1) + 5$ не являются простыми числами (последнее кратно 5, ибо, как известно, $p_2 = 101$).

(1) Этот почти единственный результат в теории распределения простых иррегулярных чисел неоднократно воспроизводился в литературе ([4], [5]). Недавно Карлиц ([6]) другим способом доказал, что простых иррегулярных чисел бесконечно много (более слабый результат!).

Числитель B_T может содержать иррегулярные числа вида $p \equiv 1 \pmod 3$ и содержит, как это следует из теоремы Вороного ([8]), простое число Q. Из сравнения Куммера

$$(*) \qquad \frac{B_T}{T} \equiv \frac{B_4}{4} \pmod{p_i}, \quad 1 \leqslant i \leqslant r,$$

следует, что иррегулярные простые числа вида $p \equiv 2 \pmod 3$, которых, по предположению, конечное число, в числитель B_T не входят. Тогда

$$(1) \qquad 3B_T \equiv 1 \pmod 3.$$

С другой стороны из обобщенного сравнения Вороного-Грюна ([9] или [10])

$$2\frac{a^m-1}{m} B_m \equiv 2 \sum_{k=1}^{N-1} (ak)^{m-1} \left[\frac{ak}{N}\right] + (1-a^m) B_{m-1} N \pmod N$$

при $(a, N) = 1$, $N > 1$, в случае, когда m, n — четные и $m \equiv n \pmod{\varphi(N)}$, вытекает сравнение типа Куммера

$$2\frac{a^m-1}{m} B_m \equiv 2\frac{a^n-1}{n} B_n \pmod N,$$

так что, в частности,

$$\frac{a^T-1}{T} B_T \equiv \frac{a^2-1}{2} B_2 \pmod 3.$$

Последнее сравнение, впрочем, следует также и из классического сравнения Вороного-Грюна

$$\frac{a^m-1}{m} B_m \equiv \sum_{k=1}^{p-1} (ak)^{m-1} \left[\frac{ak}{p}\right] \pmod p,$$

где $p \neq 2$ — простое, а m — четное число.

Если же положить $a = 2$ и учесть, что $Q \equiv 1 \pmod 3$, то придем к сравнению

$$(2^{4Q}-1) B_T \equiv 1 \pmod 3$$

или

$$15B_T \equiv 1 \pmod 3,$$

таким образом, окончательно в противоречие с (1)

$$(2) \qquad 3B_T \equiv -1 \pmod 3.$$

Итак, иррегулярных простых вида $p \equiv 2 \pmod 3$ (или, что все равно, вида $p \equiv 5 \pmod 6$) бесконечно много. Отметим также, что существуют

такие простые иррегулярные числа p, что одновременно $p \equiv 2 \pmod 3$ и $p \equiv 1 \pmod 4$, например, $p = 101$, 233 и другие.

3. Наконец, изложенное доказательство позволяет дать метод построения иррегулярных простых чисел вида $p \equiv 2 \pmod 3$. Действительно, если взять иррегулярные простые числа в некотором количестве $p_1, \ldots, p_r$, то составив простое число Q (по указанному выше закону), заметим, что (2) выполняется, а сравнение (*) справедливо лишь для p_i с $1 \leqslant i \leqslant r$ и, следовательно, в числитель B_T входит, по крайней мере, одно иррегулярное простое число $q \equiv 2 \pmod 3$, отличное от p_i, $1 \leqslant i \leqslant r$. Подобные построения возможны и в случае, рассмотренном в [3].

Очевидна аналогия с доказательством бесконечности простых чисел по Эвклиду, когда построенное из нескольких простых чисел число Эвклида имеет простой делитель, отличный от первоначально взятых.

Цитированная литература

[1] E. E. Kummer, *Allgemeiner Beweis der Fermatschen Satzes, daß die Gleichung $x^\lambda + y^\lambda = z^\lambda$ durch ganze Zahlen unlösbar ist, für alle diejenigen Potenz-Exponenten λ, welche ungerade Primzahl sind und in der Zählern der ersten $\frac{1}{2}(\lambda-3)$ Bernoullischen Zahlen als Faktoren nicht vorkommen*, J. für Math. 40 (1850), стр. 130-138.

[2] H. S. Vandiver, *On the first factor of the class-number of cyclotomic field*, Bull. Amer. Math. Soc. 25 (1919), стр. 458-461.

[3] K. L. Jensen, *Om talteoretiske Egenskaber ved de Bernoulliske Tal*, Nyt. Fidsskr. for Math. 26 (1915), стр. 73-83.

[4] H. S. Vandiver, *Examination of methods of attack on the second case Fermat's Last Theorem*, Proc. Nat. Acad. Sci., U.S.A., 40 N 8 (1954), стр. 732-735.

[5] H. S. Vandiver, *Is there an infinity of regular primes?*, Scripta Math. 21 (1955-1956), стр. 306-309.

[6] L. Carlitz, *Note on irregular primes*, Proc. Amer. Math. Soc. 5 (1954), pp. 329-331.

[7] J. L. Selfridge, C. A. Nicol, H. S. Vandiver, *Proof of Fermat's Last Theorem for prime exponents less than 4002*, Proc. Nat. Acad. Sci., U.S.A., 41 (1955), стр. 970-973.

[8] Г. Ф. Вороной, *О числах Бернулли*, Собр. соч., Киев, 1952, том I, стр. 7-23.

[9] А. А. Киселев, И. Ш. Славутский, *О числе классов идеалов квадратичного поля и его колец*, Доклады АН СССР 126 (1959), стр. 1191-1194.

[10] И. Ш. Славутский, *О числе классов идеалов вещественного квадратичного поля с простым дискриминантом*, Учен. Записки, Ленинградский Гос. Педагогический ин-т им. Герцена 218 (1961), стр. 179-189.

Reçu par la Rédaction le 29. 3. 1962