und dem arithmetischen Charakter des Systems $\alpha_1, \alpha_2, \ldots, \alpha_r$. Eine einfache obere Abschätzung von f in Abhängigkeit von

$$\gamma = \gamma(\alpha_1, \alpha_2, \ldots, \alpha_r) = \sup\{\beta > 0;\ \liminf_{k\to+\infty} P_k k^\beta < +\infty\}$$

ist in [6] gegeben. Eine gründliche Untersuchung dieser Abhängigkeit (siehe die vorläufige Mitteilung [7]) wird in einem selbstständigen Artikel behandelt.

Bemerkung 9. Wir bemerken, daß offenbar

$$A(x; Q, a_j, M_j, b_j) = A\left(t^3x; tQ, \frac{a_j}{t}, tM_j, tb_j\right)$$

($t > 0$) ist, d.h. die Ergebnisse dieser Arbeit kann man auf den Fall übertragen, daß die Zahlen

$$a_{jl},\ b_j,\ M_j \quad (j, l = 1, 2, \ldots, r)$$

ganze Vielfache einer reellen Zahl sind.

Literaturverzeichnis

[1] V. Jarník, *Über Gitterpunkte in mehrdimensionalen Ellipsoiden*, Math. Ann. 100 (1928), S. 699-721.

[2] — *Über Gitterpunkte in mehrdimensionalen Ellipsoiden*, Zweite Abhandlung, Math. Ann. 101 (1929), S. 136-146.

[3] — *Eine Bemerkung zur Gitterpunktlehre*, Časopis pro pěstování matematiky a fysiky 69 (1940), S. 57-60.

[4] — *Über die Mittelwertsätze der Gitterpunktlehre*, 5. Abhandlung, Časopis pro pěstování matematiky a fysiky 69 (1940), S. 148-174.

[5] E. Landau, *Ausgewählte Abhandlungen zur Gitterpunktlehre*, Berlin 1962.

[6] Б. Новак, *Целые точки в многомерных эллипсоидах*, ДАН СССР 153 (1963), S. 762-764.

[7] B. Novák, *On lattice points in high-dimensional ellipsoids*, Preliminary communication, Comment. Math. Univ. Carol. 7 (1966), S. 479-484.

[8] H. Petersson, *Über die Anzahl der Gitterpunkte in mehrdimensionalen Ellipsoiden*, Abh. Math. Sem., Hamburg, 5 (1926), S. 116-150.

[9] A. Walfisz, *Über Gitterpunkte in mehrdimensionalen Ellipsoiden*, Math. Zeitschrift 19 (1924), S. 300-307.

[10] — *Über Gitterpunkte in mehrdimensionalen Ellipsoiden*, Dritte Abhandlung, Math. Zeitschrift 27 (1927), S. 245-268.

[11] — (А. З. Вальфиш), *Абсциссы сходимости некоторых рядов Дирихле*, Труды Тбилисского Мат. ин. XXII (1956), S. 33-75.

[12] — *Gitterpunkte in mehrdimensionalen Kugeln*, Warszawa 1957.

[13] V. Jarník und A. Walfisz, *Über Gitterpunkte in mehrdimensionalen Ellipsoiden*, Math. Zeitschrift 32 (1930), S. 152-160.

Reçu par la Rédaction le 29. 3. 1967

ACTA ARITHMETICA
XIII (1968)

О некоторых возможностях обращения малой теоремы Ферма

М. М. Артюхов (Орджоникидзе)

В этой заметке рассматриваются вопросы такого же характера, как и в недавно опубликованной заметке [1], но результаты, полученные в той и другой, между собой независимы. Основное содержание настоящей заметки заключается в изучении одного нового аспекта обращения теоремы Ферма, в связи с чем появляются некоторые новые критерии простоты натуральных чисел.

Буква n здесь всюду будет обозначать заданное нечетное натуральное число, большее единицы, а буква A — всякое из чисел наименьшей положительной приведенной системы вычетов заданного модуля n.

В качестве основной мы примем следующую формулировку теоремы Ферма:

Если n — простое число, то каждое A удовлетворяет сравнению

$$x^{n-1} - 1 \equiv 0 \pmod{n}. \tag{F}$$

Хорошо известно, что существуют и составные числа n, обладающие этим же самым свойством. Такие числа, в отличие от простых, мы будем называть (следуя В. Серпинскому) *абсолютно псевдопростыми* (в литературе они известны также, как числа Кармайкла; наиболее полно современные сведения о них изложены в обзорной статье Е. Грассини [4]). Поскольку еще не выяснено, бесконечно или конечно множество всех абсолютно псевдопростых чисел (если допустить справедливость известной H-гипотезы А. Шинцеля [5], оно бесконечно), то теорема Ферма в указанной основной формулировке необратима даже для сколь угодно больших n. В заметке [1] установлено, что, несмотря на существование абсолютно псевдопростых чисел, своего рода „половина" теоремы Ферма обратима. Имеется в виду известное положение Эйлера о том, что,

если n — простое число, то каждый квадратичный невычет модуля n удовлетворяет сравнению

$$x^{(n-1)/2} + 1 \equiv 0 \pmod{n}. \tag{E$_1$}$$

Оказывается, что и наоборот,
если при данном n сравнению (E_1) *удовлетворяет каждый квадратичный невычет модуля n, то n — простое число.*
Более того,
если при данном n сравнению (E_1) *удовлетворяет каждое A, для которого символ Якоби $(A/n) = -1$, то n — простое число.*

Все это позволило предложить критерии простоты чисел, фигурирующие в [1] как теоремы D и E. Что касается „другой половины" теоремы Ферма, связанной со сравнением

$$(E_2) \qquad x^{(n-1)/2}-1 \equiv 0 \pmod{n},$$

то-есть, с соответствующим положением Эйлера о квадратичных вычетах простого модуля n, то она так же необратима, как и „целая" теорема Ферма.

В вышеупомянутых критериях теорема Ферма обращается лишь „наполовину", и в них так или иначе учитываются квадратичные характеры чисел A по модулю n. Поэтому имеет смысл ввести более полные обращения, обходящиеся к тому же без учета квадратичных характеров чисел.

Начнем с того факта, что теореме Ферма можно придать, например, следующую формулировку:

Если n — простое число, то каждое из чисел A удовлетворяет одному из сравнений (E_1), (E_2).

Это вполне понятно, так как $A^{n-1}-1 = (A^{(n-1)/2}+1)(A^{(n-1)/2}-1)$, и из делимости левой части этого равенства на простое число n вытекает делимость одного (и только одного) из сомножителей правой части на то же n. Оказывается, что это положение, дополненное требованием разрешимости сравнения (E_1), можно обратить, и, в целом, получить следующую теорему:

Критерий А. *Для того, чтобы n было простым числом, необходимо и достаточно, чтобы каждое A удовлетворяло одному из сравнений* (E_1), (E_2), *причем, чтобы по крайней мере в одном случае удовлетворялось сравнение* (E_1).

Этот критерий является частным случаем более общего критерия, к доказательству которого мы сейчас и переходим.

Лемма I (Р. Кармайкла [2]). *Абсолютно псевдопростое число не может делиться на квадрат простого числа.*

Лемма II. *Пусть $n = hm+1$, где $h>1$ и m — натуральные числа. Если у n имеется такой простой делитель p, что $(p-1, n-1)|m$, то сравнение $x^{(h-1)m}+x^{(h-2)m}+\ldots+x^m+1 \equiv 0 \pmod{n}$ не имеет решений.*

Доказательство. Допустим, что при условиях леммы имеется число A, удовлетворяющее указанному сравнению. Очевидно, что $(A, p) = 1$, и, значит, какой то делитель δ числа $p-1$ будет показателем, которому A принадлежит по модулю p. Вместе с тем, поскольку мы допустили, что A сравнению леммы удовлетворяет, то, в частности,

$$(1) \qquad A^{(h-1)m}+A^{(h-2)m}+\ldots+A^m+1 \equiv 0 \pmod{p},$$

откуда $A^{n-1}-1 \equiv 0 \pmod{p}$, и, следовательно, $\delta|n-1$. Сопоставляя факты: $\delta|p-1$, $\delta|n-1$ и условие леммы $(p-1, n-1)|m$, мы видим, что должно быть $\delta|m$, а это влечет за собой

$$(2) \qquad A^m-1 \equiv 0 \pmod{p}.$$

Пришли к противоречию, так как сравнение (2) несовместимо со сравнением (1) (из (2) вытекает, что $A^{(h-1)m}+A^{(h-2)m}+\ldots+A^m+1 \equiv \equiv h \pmod{p}$, но $(h, p) = 1$ из-за того, что $(h, n) = 1$).

Общий критерий. *Пусть $h>1$ и m — такие натуральные числа, что $n = hm+1$, и построим сравнения*

$$(3) \qquad x^{(h-1)m}+x^{(h-2)m}+\ldots+x^m+1 \equiv 0 \pmod{n},$$

$$(4) \qquad x^m-1 \equiv 0 \pmod{n}.$$

Тогда для того, чтобы n было простым числом, необходимо и достаточно, чтобы каждое A удовлетворяло одному из сравнений (3), (4), *причем, чтобы по крайней мере в одном случае удовлетворялось сравнение* (3).

Доказательство необходимости. Пусть n — простое число. Тогда при любом A имеем

$$A^{n-1}-1 \equiv 0 \pmod{n},$$

или, что — то же самое,

$$(A^m-1)(A^{(h-1)m}+A^{(h-2)m}+\ldots+A^m+1) \equiv 0 \pmod{n},$$

и один из сомножителей левой части этого сравнения обязан делиться на n, то-есть, A удовлетворяет одному из сравнений (3), (4). Кроме того, при любом $h>1$ у простого $n = hm+1$ имеется хотя бы один невычет h-ой степени и он обязан удовлетворять сравнению (3).

Доказательство достаточности. Если каждое A удовлетворяет одному из сравнений (3), (4), то это означает, что каждое A удовлетворяет сравнению (F), и, следовательно, n — либо простое, либо — абсолютно псевдопростое число. Осталось убедиться в том, что вторая возможность в данном случае полностью отпадает. Для этого, допустив, что n — число абсолютно псевдопростое, мы укажем сейчас такое A_0, которое не удовлетворит ни одному из сравнений (3), (4). Дело в том, что если n — абсолютно псевдопростое число и p — один из его простых делителей, то $n = pP$, где $P>1$, причем, в силу леммы I,

$(p, P) = 1$. Последнее обстоятельство обеспечивает разрешимость системы сравнений: $z \equiv g \pmod{p}$ и $z \equiv 1 \pmod{P}$, где g — какой-нибудь первообразный корень модуля p. Возьмем в качестве A_0 число, удовлетворяющее этой системе сравнений, и рассмотрим следующие числа:

$$M = A_0^{(h-1)m} + A_0^{(h-2)m} + \ldots + A_0^m + 1 \quad \text{и} \quad N = A_0^m - 1.$$

Поскольку $A_0 \equiv 1 \pmod{P}$, то $M \equiv h \pmod{P}$, и, так как $P > 1$, а $(h, P) = 1$, то $M \not\equiv 0 \pmod{P}$, а потому и $M \not\equiv 0 \pmod{n}$. Для доказательства того, что и $N \not\equiv 0 \pmod{n}$, допустим противное, то-есть, $N \equiv 0 \pmod{n}$. Из допущения сразу последует $g^m \equiv 1 \pmod{p}$, и, поскольку g — первообразный корень модуля p, то должно было бы быть $p-1 | m$. Однако этого как раз не может быть, так как по условию доказываемого критерия разрешимо сравнение (3), являющееся тем сравнением из леммы II, которое в силу самой этой леммы не может быть разрешимо при $p-1|m$ (потому что из $p-1|m$ вытекает, что и $(p-1, n-1)|m$).

Таким образом общий критерий доказан, причем мы видим, что при любых $h \geqslant 2$ и m он охватывает теорему Ферма как свою „прямую часть" и ее обращение — как „обратную часть". Правда, при этом имеется в виду несколько своеобразная формулировка самой теоремы Ферма, формулировка, в которой сравнение Ферма (F) мы „разлагаем" на два сравнения, (3) и (4).

Сформулированный ранее критерий A может быть теперь сразу получен из доказанного общего критерия, если в нем положить $h = 2$. Достоинством критерия A при его сравнении с другими частными случаями общего критерия является то, что для решения вопроса, удовлетворяет ли в конкретном случае то или иное A одному из сравнений (3), (4), достаточно найти наименьший положительный вычет по модулю n единственной степени, $A^{(n-1)/2}$, числа A, тогда как при $2 < h < n-1$ вычетом одной какой-нибудь степени числа A уже не обойтись. К недостаткам же критерия A следует отнести переходящее в него из общего критерия требование разрешимости сравнения (E_1). В связи с этим не мешает отметить, что при $n \equiv 3 \pmod{4}$ это требование из критерия A автоматически устраняется, так как у сравнения (E_1) в этом случае имеется очевидное решение, $x = n-1$.

Без требования разрешимости сравнения (3) можно обойтись не только в указанном случае, но и всегда, когда мы у $n = hm+1$ в качестве h возьмем число четное, причем так, чтобы m оказалось нечетным. В частности, имеет место следующий

Критерий B. *Если $n = 2^a k + 1$, где a и нечетное k — натуральные числа, то для того, чтобы n было простым числом, необходимо и достаточно, чтобы каждое A удовлетворяло одному из сравнений*:

$$x^{(2^a-1)k} + x^{(2^a-2)k} + \ldots + x^k + 1 \equiv 0 \pmod{n}, \qquad x^k - 1 \equiv 0 \pmod{n}.$$

Являясь частным случаем общего критерия при $h = 2^a$, $m = k$, критерий B уже не содержит требования разрешимости первого из указанных в нем сравнений так как благодаря нечетности m и четности h оно имеет очевидное решение $x = n-1$.

Как в теореме Ферма, так и в уже рассмотренных здесь критериях простоты чисел мы употребляли наименьшую положительную (что, конечно, не обязательно) приведенную (что — существенно) систему вычетов модуля n, в которую, в частности, непременно входит число $A = 1$. По отношению к $A = 1$ все эти теоремы представляются, по существу, безразличными, так как $A = 1$ является тривиальным решением сравнения $x^q - 1 \equiv 0 \pmod{n}$ при любых натуральных n и q, то-есть, во всех этих теоремах можно было бы обходиться той же приведенной системой вычетов, но без вычета $A = 1$. В связи с такой возможностью примечательно то, что как раз это число $A = 1$ и является помехой непосредственному полному обращению теоремы Ферма в основной формулировке. Сравнение (F) удовлетворяется каждым A в двух и только в двух случаях: либо, если n — простое, либо, если n — абсолютно псевдопростое число, но оказывается, что стоит только освободить это сравнение от тривиального решения $x = 1$, то-есть, поделить его на $x-1$, как новое сравнение станет удовлетворяться каждым A (теперь, конечно, — за исключением $A = 1$) лишь в первом случае. Иначе говоря, имеет место следующий критерий (в двух редакциях, эквивалентность которых очевидна).

Критерий C (первая редакция). *Для того, чтобы n было простым числом, необходимо и достаточно, чтобы каждое A, кроме $A = 1$, удовлетворяло сравнению*

$$x^{n-2} + x^{n-3} + \ldots + x + 1 \equiv 0 \pmod{n}. \tag{5}$$

Критерий C (вторая редакция). *Для того, чтобы n было простым числом, необходимо и достаточно, чтобы для каждого A, кроме $A = 1$, выполнялось условие*

$$A^{n-1} \equiv 1 \pmod{\nu}, \tag{6}$$

где $\nu = (A-1)n$.

Доказательство. Этот критерий является частным случаем предложенного выше общего критерия, получаясь из него при $m = 1$, $h = n-1$, но он же имеет и очень простое самостоятельное доказательство, обходящееся, в частности, без понятия псевдопростого числа. Необходимость условия, указанного в этом критерии, сразу следует из теоремы Ферма в основной формулировке, а для доказательства его достаточности нужно только убедиться в том, что если n — составное число, то найдется такое $A \neq 1$, которое не удовлетворит сравнению (5). Таким числом является, например, $A_0 = p+1$, где p —

наименьший простой делитель данного составного n. Действительно, во-первых, $(A_0, n) = 1$ (из-за того, что p — наименьший простой делитель числа n), во-вторых, $A_0^{n-2}+A_0^{n-3}+\ldots+A_0+1 \equiv n-1 \pmod p$, и так как $(n-1,\ p) = 1$, то A_0 не удовлетворяет сравнению (5) по модулю p, а, следовательно, и по модулю n.

Во второй из выше приведенных редакций критерия C модуль сравнения (6) выглядит несколько необычно, $\nu = (A-1)n$, то-есть, A участвует не только в сравниваемых числах, но и в модуле сравнения. Однако проверка справедливости такого сравнения для того или иного $A \neq 1$ в практическом отношении гораздо проще, чем проверка справедливости сравнения

$$A^{n-2}+A^{n-3}+\ldots+A+1 \equiv 0 \pmod n. \tag{7}$$

При проверке справедливости сравнения (6) для данных n и A можно пользоваться следующим алгорифмом:

1. Представить $n-1$ в двоичной системе счисления, $n-1 = 1a_{k-1}a_{k-2}\ldots a_1a_0$ (где все a_i — соответствующие цифры 0,1 двоичной записи $n-1$), и выписать в порядке возрастания $i_1 < i_2 < \ldots < i_l$ номера всех a_i, являющихся единицами.

2. Вычислить модуль $\nu = (A-1)n$.

3. Вычислить абсолютно наименьший по модулю ν вычет B_1 числа A^2, затем — абсолютно наименьший вычет B_2 числа B_1^2, и т.д., — до абсолютно наименьшечо вычета B_k числа B_{k-1}^2.

4. Вычислить абсолютно наименьший вычет C_2 произведения $B_{i_1}B_{i_2}$, затем — абсолютно наименьший вычет C_3 произведения $C_2B_{i_3}$, и т.д., — до абсолютно наименьшего вычета C_l произведения $C_{l-1}B_{i_l}$. В результате получим $C_l \equiv A^{n-1} \pmod \nu$.

Основной операцией этого алгорифма является перемножение двух чисел (равных, или различных), по абсолютной величине меньших, чем ν, и отыскание абсолютно наименьшего (можно, конечно, и — наименьшего положительного) остатка от деления полученного произведения на ν. Таких операций для проверки выполнимости условия (6) требуется проделать меньше, чем $2k$, то-есть, меньше, чем $2\log_2 n$. Если же прибегать к непосредственной проверке справедливости сравнения (7) при $A \neq 1$, то количество таких же операций будет иметь порядок самого числа n.

Теорему Ферма, как известно, можно расширить, не ограничиваясь в ней только числами A приведенной системы вычетов модуля n. Она остается в силе и при следующей формулировке:

Если n — простое число, то каждое целое число удовлетворяет сравнению

$$x^n \equiv x \pmod n.$$

Оказывается, что эту расширенную теорему Ферма тоже нельзя обратить непосредственно, причем, — по той же самой причине, что и теорему Ферма в основной формулировке. Дело в том, что и при всяком абсолютно псевдопростом n каждое целое число удовлетворяет сравнению (8) (см., например, [4]). Нетрудно, однако, выяснить, что все предложенные здесь критерии простоты чисел могут быть расширены в том же смысле, что и теорема Ферма. Вот, например, как можно формулировать критерий B в расширенной трактовке:

Если $n = 2^a k+1$, где a и нечетное k — натуральные числа, то для того, чтобы n было простым числом, необходимо и достаточно, чтобы каждое целое число удовлетворяло одному из сравнений:

$$x^{(2^a-1)k}+x^{(2^a-2)k}+\ldots+x^k+1 \equiv 0 \pmod n, \qquad x^{k+1} \equiv x \pmod n.$$

Необходимость введенного здесь условия вытекает из расширенной теоремы Ферма, а достаточность основана на том, что если n — составное, то (как выяснялось при доказательстве общего критерия) уже и среди взаимно простых с n чисел A найдется число, не удовлетворяющее обоим указанным здесь сравнениям.

Теперь мы уточним критерий C, так как в нем, по существу, теорема Ферма и в случае расширенной трактовки обращается наиболее полно. Для его усовершенствования понадобятся две леммы.

Лемма III. *Пусть q — простое число $\geqslant 11$, r — какой-нибудь простой делитель $q-1$, а w — наименьший положительный невычет r-ой степени по модулю q. Если $r = 2$ и $q \equiv 1 \pmod 4$, то $w < \sqrt{q/2}+\frac{1}{4}$, если же $r > 2$, то, каково бы не было q, $w < \sqrt{q/2}$.*

Доказательство. Чтобы доказать эту лемму достоточно чуть-чуть модифицировать известный способ получения простейшей оценки наименьшего положительного квадратичного невычета простого модуля (см. [3]). Прежде всего заметим, что если число 2 — невычет r-ой степени модуля q, то лемма сразу справедлива (поскольку $2 < \sqrt{11/2} \leqslant \sqrt{q/2}$), поэтому далее будем предполагать, что 2 — вычет r-ой степени модуля q, и, следовательно, w — нечетное число (оно, как известно, должно быть простым). Нечетные числа $1, 3, \ldots, w-2$ являются вычетами r-ой степени модула q, а так как -1 в рассматриваемых случаях тоже вычет r-ой степени модуля q, то и $-1, -3 \ldots, -(w-2)$ — вычеты. В совокупности те и другие составляют приведенную систему вычетов модуля $2w$ и это обеспечивает наличие среди них такого ξ, что $2w | q+\xi$. Положив $w_1 = (q+\xi)/2w$, мы видим, что w_1 является положительным невычетом r-ой степени для модуля q. В случае, когда $r > 2$, имеем $w_1 \geqslant w+2$ (так как ни w^2, ни $(w+1)w$ вычетами r-ой степени для модуля q оказаться не могут), а в случае $r = 2$ имеем $w_1 \geqslant w$, так что — в первом случае $q+w-2 \geqslant 2w^2+4w$, а во втором

$q+w-2 \geqslant 2w^2$. Из этих неравенств сразу и получаются оценки, указанные в лемме.

Лемма IV. *Для каждого нечетного простого p имеется простое $v < p^{2/3}$, не удовлетворяющее сравнению*

$$x^{p-1} \equiv 1 \pmod{p^2}. \tag{9}$$

Доказательство. Известно, что наименьшим из простых чисел p, при котором сравнению (9) удовлетворяет число 2, является $p = 1093$, поэтому для всех $p < 1093$ доказываемая лемма заведомо справедлива, и остается убедиться в ее справедливости при каждом $p \geqslant 1093$. Допустим, что для какого-нибудь $p \geqslant 1093$ все простые $v_1, v_2, \ldots, v_l$, меньшие, чем $p^{2/3}$, сравнению (9) удовлетворяют. В таком случае ему будут удовлетворять и все числа λ вида $\lambda = v_i v_j v_k$, чде i, j, k независимо друг от друга пробегают все номера $1, 2, \ldots, l$. Если обозначим через L количество всех различных λ, то, очевидно, $L > l^3/6$. Но $l = \pi(p^{2/3})$ — число простых чисел, не превосходящих $p^{2/3}$, и достаточно взять для него простейшую оценку снизу, $\pi(x) > \dfrac{x}{\log_2 x} - 2$ (полученную по совершенно упрощенной чебышевской схеме оценки $\pi(x)$ Л. Г. Шнирельманом [6]), чтобы убедиться в том, что при $p \geqslant 1093$ окажется $L > p$. Таким образом, поскольку каждое из чисел λ заключено в границах $1 < \lambda < p^2$, наше допущение, что все $v_1, v_2, \ldots, v_l$ сравнению (9) удовлетворяют, приводит к заключению о наличии у сравнения (9) более, чем p, различных решений (различных — в смысле классов чисел по модулю p^2), в действительности же, как известно, это сравнение имеет ровно $p-1$ решений. Значит допущение не корректно, и хотя бы одно не удовлетворяющее сравнению (9) простое число $v < p^{2/3}$ обязано иметься.

Понятно, что оценка сверху для v при больших p может быть значительно улучшена, но для целей заметки в этом нет нужды.

Критерий D (уточнение критерия C в расширенной трактовке). *Для того, чтобы нечетное натуральное число n было простым, необходимо и достаточно, чтобы для каждого целого числа a, удовлетворяющего неравенствам $1 < a < \sqrt[3]{n}$, выполнялось условие*

$$a^n \equiv a \big(\operatorname{mod}(a-1)n\big). \tag{10}$$

Доказательство. Необходимость условия (10) является прямым следствием из расширенной теоремы Ферма (так как при простом n имеем $(a-1, n) = 1$). Чтобы убедиться в его достаточности, мы установим, что для каждого составного n найдется a, удовлетворяющее неравенствам $1 < a < \sqrt[3]{n}$, но не удовлетворяющее условию (10).

Известно, что для всех составных $n < 341$ имеем $2^{n-1} \not\equiv 1 \pmod{n}$, и так как для всех этих n $1 < 2 < \sqrt[3]{9} \leqslant \sqrt[3]{n}$, то при $n < 341$ доказываемый критерий справедлив. Переходя к $n \geqslant 341$ далее под p и q мы будем понимать простые числа, удовлетворяющие неравенствам $3 \leqslant p < q$, и рассмотрение всех составных $n \geqslant 341$ разобьем на 4 варианта

a) $n = pq$, где $q < p^2+4p$.

b) $n = p^2 s$, где s — нечетное натуральное число, причем $s \neq p$ и $1 < s < 2p-1$.

c) $n = p^a$, где натуральное $a \geqslant 2$.

d) $n = pt$, где натуральное $t \geqslant p^2+4p$.

Нетрудно усмотреть, что эти варианты охватывают (частично перекрываясь) все подлежащие рассмотрению составные нечетные $n \geqslant 341$, так как в варианте d) учитываются: неучтенная в a) возможность $q > p^2+4p$ и неучтенная в b) возможность $s \geqslant 2p-1$; а, кроме того, в c) учитывается возможность $s = p$, исключенная из b).

Займемся этими вариантами поочередно.

a) При $n = pq \geqslant 341$ и $p < q$ должно быть $q \geqslant 23$, а к таким q применима лемма III, которую здесь можно использовать следующим образом. Из $n-1 = (p-1)(q-1)+(p-1)+(q-1)$ и $p < q$ вытекает, что $q-1 \nmid n-1$. Следовательно, хотя бы одно простое r входит в каноническое разложение числа $q-1$ в более высокой степени, чем в каноническое разложение числа $n-1$ (при этом, если $r = 2$, то обязательно будет $q \equiv 1 \pmod{4}$). По лемме III у q найдется положительный невычет r-ой степени, w, удовлетворяющий неравенству $w < \sqrt{q/2}+\frac{1}{4}$. Известно же, что показатель, которому такое число принадлежит по модулю q, должен делиться на максимальную степень числа r, входящую в каноническое разложение числа $q-1$, и так как $n-1$ на эту степень r не делится, то $w^{n-1} \not\equiv 1 \pmod{q}$, значит, и подавно, $w^{n-1} \not\equiv 1 \pmod{n}$. Вместе с тем нетрудно проверить, что при $p < q < p^2+4p$ и $q \geqslant 23$ из $w < \sqrt{q/2}+\frac{1}{4}$ следует $w < \sqrt[3]{n}$.

b) В этом варианте из $s \neq p$ и $1 < s < 2p-1$ вытекает, что $p-1 \nmid n-1$, так что при $p \geqslant 11$ здесь таким же путем, как и в a) приходим к заключению о наличии такого w, что $1 < w < \sqrt[3]{n}$, но $w^{n-1} \not\equiv 1 \pmod{n}$. При всех же $p < 11$ здесь выясняется, что $2^{n-1} \not\equiv 1 \pmod{n}$.

c) Для всех n из этого варианта имеем $\big(n-1, \varphi(n)\big) = p-1$. Поэтому, если для какого-нибудь a оказывается $a^{n-1} \equiv 1 \pmod{n}$, то, поскольку, кроме того, $a^{\varphi(n)} \equiv 1 \pmod{n}$, обязательно будет $a^{p-1} \equiv 1 \pmod{n}$, и так как $p^2 | n$, то получим $a^{p-1} \equiv 1 \pmod{p^2}$. Но по лемме IV для p имеется большее единицы число $v < p^{2/3} \leqslant n^{1/3}$ такое, что $v^{p-1} \not\equiv 1 \pmod{p^2}$, и, следовательно, $v^{p-1} \not\equiv 1 \pmod{n}$.

d) В этом варианте в качестве нужного a всегда можно взять $a=p+1$. Действительно, $(a-1, a^{n-1}+a^{n-2}+\ldots+a^2+a)=1$, и так как $a-1=p$, то $a^{n-1}+a^{n-2}+\ldots+a^2+a$ на $n=pt$ делиться не может. Вместе с тем, при условиях этого варианта имеем $p+1<\sqrt[3]{n}$.

Рассмотрев все возможности, мы убедились, что при любом нечетном составном n найдется целое a, удовлетворяющее неравенствам $1<a<\sqrt[3]{n}$, для которого $(a-1)n\nmid a^n-a$. Тем самым справедливость критерия D полностью обоснована.

Так как при доказательстве критерия D в качестве a из леммы III берется w, а из леммы IV — берется v, оба являющиеся простыми числами, и так как в варианте d) берется $a=p+1$, где p — простое, то критерий D можно формулировать и в следующей еще более уточненной редакции:

Для того, чтобы нечетное натуральное число n было простым, необходимо и достаточно, чтобы условие (10) *выполнялось для всех a, удовлетворяющих неравенствам $1<a<\sqrt[3]{n}$ и являющихся либо простыми числами, либо числами большими простых на единицу.*

В заключение следует отметить, что существенно улучшить верхнюю границу для чисел a в критерии D не представляется возможным. Дело в том, что если n — абсолютно псевдопростое число вида $n=pqr$, где $p<q<r$ — простые числа (а такие абсолютно псевдопростые имеются, причем неизвестно, конечно или бесконечно их множество), то наименьшим положительным a, для которого условие (10) не осуществляется, будет $a=p+1$.

Цитированная литература

[1] М. М. Артюхов, *Некоторые критерии простоты чисел, связанные с малой теоремой Ферма*, Acta Arith. 12 (1967), стр. 355-364.

[2] R. D. Carmichael, *On composite numbers p which satisfy the Fermat congruence* $a^{p-1}\equiv 1 \pmod p$, Amer. Math. Monthly 19 (1912), стр. 22-27.

[3] А. О. Гельфонд и Ю. В. Линник, *Элементарные методу в аналитической теории чисел*, Москва 1962, стр. 217.

[4] E. Grassini, *I numeri composti m che verificano la congruenza* $a^{m-1}\equiv 1 \pmod m$, Period. Mat. 43 (1965), стр. 183-208.

[5] A. Schinzel et W. Sierpiński, *Sur certains hypothèses concernant les nombres premiers*, Acta Arith. 4 (1958), стр. 185-208.

[6] Л. Г. Шнирельман, *Простые числа*, Москва-Ленинград 1940, стр. 46-50.

Reçu par la Rédaction le 29. 3. 1967