над вполне вещественным полем K не превышает 1, то кривая

$$x^6+y^6 = A$$

за исключением случаев: $A = 1, \{x, y\} = \{\pm 1, 0\}, \{0, \pm 1\}$; $A = 2, \{x, y\} = \{\pm 1, \pm 1\}$ *в этом поле точек не имеет.*

В заключение, выражаю глубокую благодарность И. Р. Шафаревичу за ряд ценных замечаний, касающихся этой работы.

Цитированная литература

[1] L. J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*, Proc. Cambridge Philos. Soc. (1922), стр. 179-192.

[2] A. Weil, *Sur un théorème de Mordell*, Bull. Sci. Math. (2) 54 (1930), стр. 182-191.

[3] G. Billing, *Beiträge zur arithmetischen Theorie ebenen kubischen Kurven vom Geschlecht eins*, Nove acta regiae Societatis Scientiarum Upsaliensis, Ser. 4, 11 (1938), стр. 1-165.

[4] В. Д. Подсыпанин, *О неопределенном уравнении* $x^3 = y^2+Az^6$, Мат. сб. 24. 3 (1949), стр. 391-405.

[5] L. E. Dickson, *History of the theory of numbers*, vol. II, Washington 1920.

Reçu par la Rédaction le 20. 5. 1966

ACTA ARITHMETICA
XII (1967)

Некоторые критерии простоты чисел, связанные с малой теоремой Ферма

М. М. Артюхов (Орджоникидзе)

Основные результаты в задачах, относящихся к обращению теоремы Ферма, были сообщены ранее Крайчиком [1] и Лемером [2], [3]. В 1957 году Робинсон [4] опубликовал доказательство довольно своеобразной теоремы, формулировку которой я здесь приведу в следующей редакции:

Пусть даны: *натуральное число* $a > 1$, *нечетное натуральное число* $m < 3\cdot 2^{a+1}$, $n = 2^a m+1$, *и пусть* ω — *какое нибудь целое число, для которого символ Якоби* $\left(\frac{\omega}{n}\right) = -1$. *Для того, чтобы* n *было простым числом, необходимо и достаточно, чтобы* $n \mid \omega^{(n-1)/2}+1$.

Применимость теоремы Робинсона весьма ограничена условием $m < 3\cdot 2^{a+1}$, поскольку при каждом данном a имеется не более, чем $3\cdot 2^a$ чисел n, допускающих испытание на простоту с помощью этого критерия. В связи с этим я предлагаю здесь несколько теорем, одни из которых приложимы при каждом фиксированном a к сколь угодно большим числам $n = 2^a m+1$ некоторых специальных видов, другие — имеют более универсальный характер.

Основные обозначения. a, h и ω будем считать заданными натуральными числами, причем h — нечетным, а $\omega > 1$. Полагаем $n = 2^a hk+1$, где k до наложения на него специальных условий будет любым нечетным натуральным числом, при котором $(n, \omega) = 1$. Для краткости еще положим $\omega^{h2^{a-1}} = a$ и $a^{k-1}-a^{k-2}+\ldots+a^2-a+1 = N$. Символ $\left(\frac{\omega}{n}\right)$ всюду будет употребляться как символ Якоби.

Лемма 1 (Эйлера). 1-ая формулировка: *Если* p *простое число и* ω — *квадратичный невычет модуля* p, *то* $p \mid \omega^{(p-1)/2}+1$.

2-ая формулировка: *Если* $\left(\frac{\omega}{n}\right) = -1$, *то при* n *простом* $n \mid \omega^{(n-1)/2}+1$.

Лемма 2. *Если у n имеется хотя бы один простой делитель $\nu = 2^\beta s+1$, такой, что s — нечетно, а $\beta < \alpha$, то $n \nmid \omega^{(n-1)/2}+1$ при любом ω.*

Доказательство. Если допустим, что $n|\omega^{(n-1)/2}+1$, и обозначим буквой δ показатель, к которому принадлежит число ω по модулю ν, то, с одной стороны, будет $\delta|2^\alpha hk$ (так как $\nu|n|\omega^{(n-1)/2}+1|\omega^{n-1}-1$), с другой $\delta|2^\beta s$. Отсюда, поскольку $\beta < \alpha$, а s нечетно, заключаем, что $\delta|2^{\alpha-1}hk = (n-1)/2$. Значит должно быть $\nu|\omega^{(n-1)/2}-1$, что несовместимо с $\nu|\omega^{(n-1)/2}+1$.

Лемма 3. *Если у n имеется хотя бы один простой делитель $\nu = 2^\beta s+1$, такой, что $(s, k) = 1$, то $\nu \nmid N$ при любом ω.*

Доказательство. Если допустим, что $\nu|N$, и обозначим буквой δ показатель числа ω по модулю ν, то так же, как и при доказательстве леммы 2, обнаружим, что одновременно и $\delta|2^\alpha hk$, и $\delta|2^\beta s$. Отсюда, поскольку в данном случае $(s, k) = 1$, следует, что $\delta|2^\alpha h$, и, значит, мы приходим к выводу, что $\nu|a^2-1$ при условии $\nu|N$, так что $\nu|(N, a^2-1)$. Но $(N, a^2-1) = (N, a+1)$ (из-за того, что $(N, a-1) = 1$), а так как $N = ka^{k-1}-(a+1)[(k-1)a^{k-2}-(k-2)a^{k-3}+\ldots+2a-1]$, то $(N, a+1) = (k, a+1)|k$. В итоге получаем $\nu|k$, что несовместимо с $\nu|n$.

Лемма 4. *Если n можно разложить на множители $(2^\beta s+1)(2^\gamma t+1) = n$, где s и t — нечетные натуральные числа, то $(s, k) = (t, k)$, причем имеет место одна и только одна из следующих двух ситуаций*:

Ситуация 1: $\beta = \gamma < \alpha$.

Ситуация 2: $\beta \neq \gamma$, $\min[\beta, \gamma] = \alpha$ *и* $2^{\alpha+1}st < kh$.

Эта лемма является результатом рассмотрения имеющего здесь место равенства:

$$2^{\beta+\gamma}st+2^\beta s+2^\gamma t = 2^\alpha hk. \tag{1}$$

Лемма 5. *При натуральных $\alpha, \sigma, \tau, p, h \leqslant 2^{\alpha-1}$ не может осуществляться равенство $2^\alpha\sigma\tau p+\sigma+\tau = hp^2$.*

Доказательство. Квадратное уравнение $hx^2-2^\alpha\sigma\tau x-(\sigma+\tau) = 0$ при $h \leqslant 2^{\alpha-1}$ и натуральных σ, τ в поле рациональных чисел неприводимо, так как его дискриминант $\Delta = (2^{\alpha-1}\sigma\tau)^2+h(\sigma+\tau)$ при этих условиях удовлетворяет неравенствам $(2^{\alpha-1}\sigma\tau)^2 < \Delta < (2^{\alpha-1}\sigma\tau+1)^2$ и потому не может быть квадратом целого числа.

Лемма 6. *При натуральных σ, τ, θ и простом $p > 2^{2\theta-1}$ не может осуществляться равенство $2^{4\theta}\sigma\tau p+\sigma+\tau = p^3$.*

Доказательство. Если допустить, что это равенство осуществляется, то это будет означать, что $\sigma+\tau = pl$, где l — число натуральное, причем $l = p^2-2^{4\theta}\sigma\tau$, так что $\sigma\tau = (p^2-l)/2^{4\theta}$. Значит σ и τ должны быть натуральными корнями квадратного относительно z уравнения $2^{4\theta}z^2-2^{4\theta}plz+p^2-l = 0$, а потому дискриминант этого уравнения $\Delta = 2^{4\theta}[(2^{2\theta-1}pl)^2-p^2+l]$ должен оказаться квадратом целого числа. Следовательно, квадратом целого должно быть и число $(r^2-1)p^2+l$, где $r = 2^{2\theta-1}l$. Положив $D = r^2-1$, мы видим, что уравнение $x^2-Dy^2 = l$ должно иметь целочисленное решение $x = x_0, y = p$, причем $(x_0, p) = 1$ (так как из $p^2-l = 2^{4\theta}\sigma\tau > 0$ вытекает, что l делиться на p^2 не может. Разлагая $\sqrt{D}$ в непрерывную дробь, получим $[r-1; \{1, 2(r-1)\}, \ldots]$ (в фигурных скобках находится основной период дроби), а по этому разложению известным способом можно легко убедиться в том, что при $l > 1$ рассматриваемое уравнение Пелля в числах, удовлетворяющих условию $(x, y) = 1$, неразрешимо. В случае же $l = 1$ для x получается условие $x^2-1 = (2^{4\theta-2}-1)p^2$, которое при простом $p > 2$ может иметь место только если либо $x+1$, либо $x-1$ делится на p^2, но такая возможность исключена условием $p > 2^{2\theta-1}$, так что лемма доказана.

Лемма 7. *При натуральных θ, σ, τ и нечетном простом p удовлетворяющем условию $2^{2\theta+2} \nmid p^2-1$, не может осуществляться равенство $2^{2\theta+1}\sigma\tau p+\sigma+\tau = p^3$.*

Доказательство. Здесь сразу отпадает возможность $\sigma+\tau = p$, поскольку это означает, что одно из чисел σ, τ должно быть четным, и, следовательно, равенство $2^{2\theta+1}\sigma\tau+1 = p^2$ окажется противоречащим условию $2^{2\theta+2} \nmid p^2-1$. Если же предполагать, что $\sigma+\tau = pl$, где натуральное $l > 1$, то допущение возможности равенства, указанного в лемме, приводит к разрешимости в целых взаимно простых числах уравнения Пелля $x^2-Dy^2 = 2l$, где $D = r^2-2$, при $r = 2^\theta l$. Отсюда будет вытекать разрешимость уравнения $x^2-Dy^2 = l$ (так как уравнение $x^2-Dy^2 = 2$ имеет очевидное решение $x = r, y = 1$). Однако, как и в лемме 6, здесь $l/\sqrt{D} < 1$, так что тем же способом, но теперь по разложению $\sqrt{D} = [r-1; \{1, r-2, 1, 2(r-1)\}, \ldots]$, можно убедиться в том, что в действительности полученное уравнение Пелля во взаимно простых числах неразрешимо.

Лемма 8. *При натуральных σ, τ и нечетном простом p, не может осуществляться равенство $2\sigma\tau p+\sigma+\tau = p^3$.*

Доказательство. В этои случае соответвующее уравнение Пелля имеет вид $x^2-Dy^2 = 2l$, где $D = l^2-2$ и l— нечетное натуральное число. Возможность $l = 1$ сразу исключается (из-за того, что не может быть $x^2+p^2 = 2$), а при $l > 1$ доказательство неразрешимости этого уравнения во взаимно простых числах проходит почти так же, как и в предыдущих случаях, правда, некоторые осложнения вызывает то, что здесь $l/\sqrt{D} > 1$.

В следующих далее теоремах A и B, будут считаться данными натуральные числа: a, нечетное h и $\omega > 1$. В формуле для

n, $n = 2^a hk+1$, k будет принимать любые натуральные нечетные значения тех видов, какие будут указаны, и будет предполагаться что для n выполняются „ω-условия", состоящие в следующем:

1. $\left(\frac{\omega}{n}\right) = -1$.
2. $n \nmid \omega^{h2^{a-1}}+1$

(ясно, что условие 2 при $n > \omega^{h2^{a-1}}+1$ выполняется автоматически).

Теорема А. *Если при данном ω выполняются ω-условия для $n = 2^a hpq+1$, где $h < 2^{a+1}$, а p и q — нечетные простые, удовлетворяющие условию*

$$\frac{hp}{2^{a+1}} < q < \frac{2^{a+1}p}{h}, \tag{2}$$

то для того, чтобы n было простым числом, необходимо и достаточно, чтобы $n \mid \omega^{(n-1)/2}+1$.

Доказательство. Необходимость этого критерия следует из леммы 1 (во второй формулировке). Для доказательства достаточности допустим, что число n делит $\omega^{(n-1)/2}+1$, но является составным. Так как по 2-му из ω-условий $n \nmid \omega^{h2^{a-1}}+1$, то из $n \mid \omega^{(n-1)/2}+1$ вытекает, что у n имеется хотя бы один простой делитель $\nu < n$, на который делится N. Пусть $\nu = 2^\beta s+1$, где s — нечетно, и пусть $n = (2^\gamma t+1)\nu$, где t — также нечетно. Ситуация 1 из леммы 4 здесь не может иметь места, так как при ней в силу леммы 2 N на ν не делится. Перейдя же к ситуации 2 и положив $(s, pq) = d$, мы должны учитывать четыре гипотетические возможности: $d = pq$, $d = p$, $d = q$, $d = 1$. Первые три возможности отпадают, так как приводят к противоречию с леммой 4 (во всех трех случаях из-за условия (2) оказывается $2^{\alpha+1}st \geqslant 2^{\alpha+1}d^2 > hpq$).

Что же касается четвертой возможности, то при ней вступает в силу лемма 3, согласно которой N не может делиться на ν.

Теорема В. *Пусть p — нечетное простое, θ-натуральное число и n имеет одну из следующих форм:*

1. $n = 2^a hp+1$, *где* $h < 2^{a+1}p$;
2. $n = 2^a hp^2+1$, *где* $h < 2^{a+1}$;
3. $n = 2^a hp^3+1$, *где* $h \leqslant 2^{a-1}$;
4. $n = 2^{4\theta}p^4+1$, *где* $p > 2^{2\theta-1}$;
5. $n = 2^{2\theta+1}p^4+1$, *где* $2^{2\theta+2} \nmid p^2-1$;
6. $n = 2p^4+1$,

и пусть при некотором ω для n выполняются ω-условия (для последних трех форм числа n при $h = 1$). В таком случае для того, чтобы n было простым числом, необходимо и достаточно, чтобы $n \mid \omega^{(n-1)/2}+1$.

Доказательство. Для n первой формы теорема доказывается так же, как и теорема А. Вторую форму n можно рассматривать как частный случай (при $p = q$) формы n в теореме А. Для n третьей формы почти все доказательство проходит так же, как для теоремы А, и только особо надо рассмотреть возможность $(s, p^3) = p$ при ситуации 2 из леммы 4. Несостоятельность этой возможности обнаруживается после перехода (путем деления на p) от соответствующего ей равенства (1) к равенству $2^\alpha \sigma\tau p+\sigma+\tau = hp^2$ (где $\sigma = \frac{s}{p}2^{\beta-\alpha}$, $\tau = \frac{t}{p}$ и в (1) для определенности принято $\beta > \gamma$, а потому $\gamma = \alpha$). Такое равенство при натуральных $\alpha, \sigma, \tau, p, h \leqslant 2^{\alpha-1}$ не может иметь места из-за леммы 5.

В случае четвертой формы n доказательство в целом такое же, как и в предыдущих случаях, и специального исследования в нем требует только вариант, когда $(s, p^4) = p$. Неосуществимость этого варианта обнаруживается после перехода от соответствующего ему равенства (1) к равенству

$$2^{4\theta}\sigma\tau p+\sigma+\tau = p^3$$

(где $\sigma = \frac{s}{p}2^{\beta-4\theta}$, $\tau = \frac{t}{p}$ и в (1) для определенности принято $\beta > \gamma$). Такое равенство в силу леммы 6 неосуществимо при натуральных θ, σ, τ и простом $p > 2^{2\theta-1}$.

Наконец, в случаях пятой и шестой форм числа n особому рассмотрению подлежит такой же вариант, как и в предыдущем случае, но и здесь появляются соответствующие равенства, несостоятельность которых доказана в леммах 7 и 8.

Можно легко усмотреть, что теорема В не распространима на числа n формы $n = 2^{4\theta+2}p^4+1$, но к таким n ее и применять не требуется, поскольку заранее известно, что все они — числа составные:

$$2^{4\theta+2}p^4+1 = (2^{2\theta+1}p^2+2^{\theta+1}p+1)(2^{2\theta+1}p^2-2^{\theta+1}p+1).$$

Особо отмечу, что те же соображения, какие применяются здесь при доказательстве достаточности критерия, заключенного в теореме А, могут быть без каких нибудь осложнений использованы для доказательства следующей теоремы о максимальном числе простых в разложении данного числа n на множители.

Теорема С. *Пусть $n = 2^a hk+1$, p — наименьший простой делитель нечетного числа k и пусть ω — число, удовлетворяющее условиям:* $\left(\frac{\omega}{n}\right) = -1$, $(n, \omega^{h2^{a-1}}+1) = 1$. *Если при этом $n \mid \omega^{(n-1)/2}+1$, то n разлагается не более, чем на $[(\log n)/\log 2^a p]$ простых сомножителей (не обязательно — различных).*

Что касается практической применимости предложенных теорем к испытанию на простоту больших чисел n рассмотренных видов, то в пользу такой возможности свидетельствуют, в частности, следующие соображения.

1. Если ω, при котором для заданного n выполняются ω-условия, известно, то для того, чтобы установить, будет ли $n|\omega^{(n-1)/2}+1$, требуется, как нетрудно подсчитать, менее, чем $2\log_2 n$ операций, каждая из которых заключается в перемножении двух натуральных чисел, меньших чем n, и отыскании наименьшего остатка от деления полученного произведения на n.

2. Если при заданных n и $\omega < n$ требуется выяснить, будет ли $\left(\frac{\omega}{n}\right) = -1$, то, поскольку $\left(\frac{\omega}{n}\right)$ — символ Якоби, его значение можно вычислить и не зная заранее, окажется ли n простым, или составным числом. Достаточно для этого применить известный алгорифм, вытекающий из квадратичного закона взаимности, распространенного на символ Якоби. Главной составной частью этого алгорифма служит алгорифм Евклида для отыскания ОНД двух чисел, и по ходу его применения может, в частности, обнаружиться, что $(n, \omega) > 1$, откуда сразу будет явствовать, что n число составное.

3. Для наперед заданных нечетных ω всегда можно заранее указать все те арифметические прогрессии $y_x = 4\omega x + \varrho$ $(x = 0, 1, 2, \ldots)$, члены которых при любых x удовлетворяют условию $\left(\frac{\omega}{y_x}\right) = -1$. Для этого только надо найти все ϱ $(1 < \varrho < 4\omega, (\varrho, 2\omega) = 1)$, у которых $\left(\frac{\varrho}{\omega}\right) = -1$, если $\omega \equiv 1 (\mathrm{mod}\, 4)$, и $\left(\frac{\varrho}{\omega}\right) \equiv -\varrho (\mathrm{mod}\, 4)$, если $\omega \equiv -1 (\mathrm{mod}\, 4)$. Например, при $\omega = 3$ это будут следующие две прогрессии: $12x+5$ и $12x+7$, а при $\omega = 5$ — четыре прогрессии:

$$20x+3, \quad 20x+7, \quad 20x+13, \quad 20x+17.$$

4. Наконец, не следует упускать из виду возможность варьировать у числа $n = 2^a m + 1$ представления нечетного m (если оно — не простое) в виде произведения $m = hk$ (с учетом и того обстоятельства, что в рассмотренных теоремах нигде не требовалось, чтобы $(h, k) = 1$).

Число ω до сих пор везде предполагалось нечетным из-за того, что при любом $a \geqslant 3$ для всякого четного $\omega = 2^u(2v+1)$ окажется

$$\left(\frac{\omega}{n}\right) = \left(\frac{2v+1}{n}\right).$$

Однако при $a = 1, 2$ в качестве ω можно употреблять и четные числа, в частности при этих a всегда можно полагать $\omega = 2$, даже, если $\left(\frac{2}{n}\right) = 1$ (что может получаться при $a = 1$, но не при $a = 2$). Теоремы A и B для таких a и $\omega = 2$ превращаются в следующие частные критерии:

Следствие I. *Пусть $n = 2hpq+1$, где $h = 1, 3$, а p и q — нечетные простые числа, для которых $hp/4 < q < 4p/h$. Тогда для того, чтобы n было простым числом, необходимо и достаточно, чтобы $n|2^{n-1}-1$.*

Следствие II. *Пусть p — нечетное простое, а n — число одного из следующих четырех видов:*

1. $n = 2hp+1$, *где* $h < 4p$ *и* $n \nmid 2^{2h}-1$;
2. $n = 2hp^2+1$, *где* $h = 1, 3$;
3. $n = 2p^3+1$;
4. $n = 2p^4+1$.

Тогда для того, чтобы n было простым, необходимо и достаточно, чтобы $n|2^{n-1}-1$.

Следствие III. *Пусть $n = 4hpq+1$, где $h = 1, 3, 5, 7$, а p и q — нечетные простые, для которых $hp/8 < q < 8p/q$. Тогда для того, чтобы n было простым числом, необходимо и достаточно, чтобы $n|2^{(n-1)/2}+1$.*

Следствие IV. *Пусть p — нечетное простое, а n — число одного из следующих трех видов:*

1. $n = 4hp+1$, *где* $h < 8p$ *и* $n \nmid 2^{2h}+1$;
2. $n = 4hp^2+1$, *где* $h = 1, 3, 5, 7$;
3. $n = 4p^3+1$.

Тогда для того, чтобы n было простым необходимо и достаточно, чтобы $n|2^{(n-1)/2}+1$.

Теперь речь пойдет о критериях более универсальных, чем предложенные выше. Хорошо известно, что необходимое условие простоты числа n, заключающееся в теореме Ферма (если n—простое, то каково бы не было взаимнопростое с ним число a, для него $n|a^{n-1}-1$), нельзя непосредственно обратить в достаточное (существуют числа Кармайкла!). Вместе с тем оказывается, что такая возможность имеется для леммы 1 Эйлера как в 1-ой, так и во 2-ой формулировках.

Теорема D. *Для того, чтобы нечетное число n было простым необходимо и достаточно, чтобы для любого квадратичного невычета ω модуля n выполнялось условие $n|\omega^{(n-1)/2}+1$.*

Доказательство. Так как необходимость этого условия следует из леммы 1 (в 1-ой формулировке), остается убедиться в том, что если n — какое угодно нечетное составное число, у него найдется

хотя бы один такой квадратичный невычет ω, что $n\nmid\omega^{(n-1)/2}+1$. Начнем со случая, когда $n=p^\lambda$ где p — нечетное простое и $\lambda\geqslant 2$. Как известно, у всякого такого n имеются первообразные корни, причем каждый из них служит квадратичным невычетом модуля n. Пусть ω — один из этих корней модуля p^λ. Поскольку $\varphi(p^\lambda)=p^\lambda-p^{\lambda-1}$, то

$$\omega^{(p^\lambda-p^{\lambda-1})/2}\equiv -1(\mathrm{mod}\,p^\lambda)$$

и с этим сравнением как раз несовместимо сравнение

$$\omega^{(p^\lambda-1)/2}\equiv -1(\mathrm{mod}\,p^\lambda)$$

(при допущении, что и это сравнение имеет место, из обоих сравнений сразу вытекало бы, что

$$\omega^{p-1}\equiv 1(\mathrm{mod}\,p^\lambda),$$

тогда как для первообразного по модулю p^λ корня ω при $\lambda\geqslant 2$ это невозможно). Осталось рассмотреть случай, когда у n имеются хотя бы два различных простых делителя p, q. В этом случае в качестве ω возьмем число, являющееся решением системы сравнений

$$\omega\equiv 1(\mathrm{mod}\,p),$$
$$\omega\equiv \varrho(\mathrm{mod}\,q),$$

где ϱ—какой-нибудь квадратичный невычет модуля q. Будучи квадратичным невычетом модуля q число ω будет квадратичным невычетом модуля n, но для этого ω сравнение $\omega^{(n-1)/2}\equiv -1(\mathrm{mod}\,n)$ как раз не имеет места, поскольку из него вытекает $\omega^{(n-1)/2}\equiv -1(\mathrm{mod}\,p)$, что противоречит принятому условию $\omega\equiv 1(\mathrm{mod}\,p)$. Теорема доказана.

Можно учитывать не все квадратичные невычеты ω составного модуля n, а только те, для которых $\left(\frac{\omega}{n}\right)=-1$, и доказать теорему, соответствующую этой постановке вопроса:

Теорема E. *Для того, чтобы не являющееся квадратом целого числа нечетное число n было составным, необходимо и достаточно, чтобы имелось хотя бы одно число ω, для которого* $\left(\frac{\omega}{n}\right)=-1$, *но* $n\nmid\omega^{(n-1)/2}+1$.

Доказательство. Достаточность указанного здесь условия вытекает из леммы 1 (во 2-ой формулировке). При доказательстве необходимости применимы те же соображения, что и в доказательстве достаточности условия из теоремы D, только здесь надо уже учитывать все различные простые делители $p_1, p_2, \ldots, p_\nu$ числа n. По крайней мере один из них (для определенности, p_ν) будет входить в каноническое разложение числа n в нечетной степени, и в качестве ω здесь можно взять решение системы сравнений

$$\begin{cases}\omega\equiv 1(\mathrm{mod}\,p_1p_2\ldots p_{\nu-1}),\\ \omega\equiv\varrho(\mathrm{mod}\,p_\nu),\end{cases}$$

где ϱ — какой-нибудь квадратичный невычет модуля p_ν. В результате получится $\left(\frac{\omega}{n}\right)=-1$, но $n\nmid\omega^{(n-1)/2}+1$.

В теореме E исключаются из рассмотрения числа n, представляющие собой квадраты целых, так как для них, в силу определения символа Якоби, вообще не существует таких ω, у которых $\left(\frac{\omega}{n}\right)=-1$.

Не надо думать, что критерии, о которых трактуют теоремы D и E, являются сугубо теоретическими и полностью неприемлемы при испытаниях на простоту больших чисел. Дело в том, что благодаря леммам 2 и 3, для большинства составных чисел, уже взяв первое попавшееся ω, у которого $\left(\frac{\omega}{n}\right)=-1$, мы обнаружим, что $n\nmid\omega^{(n-1)/2}+1$, то-есть, заключим, что n — число составное. Если же для $n=2^\alpha m+1$ (где m — нечетно) взять такое ω, что $\left(\frac{\omega}{n}\right)=-1$, а $(n,\omega^{2^{\alpha-1}}+1)=1$, то противоположный результат, $n|\omega^{(n-1)/2}+1$, вообще будет получаться в тех и только тех случаях, когда n — либо само число простое, либо каждый его простой делитель имеет форму $2^\beta\mu+1$, где $\beta\geqslant\alpha$ и $(\mu,m)>1$. Последнее обстоятельство позволяет далее испытывать n путем его деления на простые указанной формы.

В заключение отмечу, что результаты, публикуемые в этой заметке, могут быть соответствующим образом использованы и в задачах, связанных с псевдопростыми числами. Нетрудно, например, из следствий 1 и 2 извлечь заключение о несуществовании чисел Пуле следующих пяти видов:

1. $n=2hpq+1$, где $h=1,3$, а p и q — нечетные простые числа, для которых $hp/4<q<4p/h$;
2. $n=2hp+1$, где $h<4p$ и $n\nmid 2^{2h}-1$;
3. $n=2hp^2+1$, где $h=1,3$;
4. $n=2p^3+1$;
5. $n=2p^4+1$.

Точно так же, о числах тех видов, какие перечисляются в следствиях 3 и 4, можно заключить, что для того, чтобы то или иное из этих чисел было числом Пуле, необходимо и достаточно, чтобы $n|2^{n-1}-1$, но $n\nmid 2^{(n-1)/2}+1$.

Цитированная литература

[1] Kraitchik, *Théorie des nombres*, tome II, стр. 133-143 (1926).

[2] D. H. Lehmer, *On the converse of Fermat's theorem*, Amer. Math. Monthly 43 (1936), стр. 347-354.

[3] — *A factorization theorem applied to a test for primality*, Bull. Amer. Math. Soc. 45 (1939), стр. 132-137.

[4] R. M. Robinson, *The converse of Fermat's theorem*, Amer. Math. Monthly 64. 10 (1957), стр. 703-710.

Reçu par la Rédaction le 18. 8. 1966

ACTA ARITHMETICA
XII (1967)

On certain additive functions

by

P. D. T. A. Elliott (Nottingham)

Towards the end of chapter 9 in his book [9] on the applications of probability to number theory, J. Kubilius proves a result which includes the following:

Let $\nu(m)$ denote the number of distinct prime divisors of a positive integer m. Let $\varepsilon_x \to 0$ as $x \to \infty$. Then for a constant $c_1 > 0$,

$$\sum_{\substack{m \leqslant x \\ |\nu(m) - \log\log x| > \varepsilon_x \log\log x}} 1 < x \exp(-c_1 \varepsilon_x^2 \log\log x). \tag{1}$$

Obviously we can rewrite this as follows:

Let $0 < a_1 < a_2 < \dots$ be a sequence of integers which in the usual notation [1] satisfies $A(x) > x\exp(-\varepsilon_x \log\log x)$. Then $\nu(a_i)$ is normally $\log\log a_i$.

This result is, in a certain sense, best possible as can be seen by taking $a_i = p_i$, the ith rational prime. This shows that we cannot replace $\varepsilon_x \to 0$ by $\varepsilon_x = 1$; in fact, it is not difficult to construct sequences A satisfying $A(x) > c_2 x (\log x)^{-\alpha}$ for any given α with $0 < \alpha < 1$, for which $\nu(a_i)$ has no normal value. We give such an example later.

Broadly speaking, the accuracy of (1) is obtained by considering the appropriate Dirichlet series and evaluating, for an appropriate range of z, the sum

$$\sum_{m \leqslant x} z^{\nu(m)}. \tag{2}$$

The evaluation of this sum was first carried out in detail by A. Selberg [13]. In this respect $\nu(m)$ enjoys distinct advantages over other functions. Essentially this is because the value of $\nu(p^\alpha)$ is the same for all powers of primes p and so can be interpreted in terms of counting functions [2].

In this present note we seek to generalise (1) to cover more general additive functions. In particular, we consider $\nu(m)$ when m runs through

[1] $A(x)$ denotes the number of $a_i \leqslant x$.

[2] Cf. the remarks near the beginning of the proof of Theorem 2.