АКАДЕМИЯ НАУК
СОЮЗА СОВЕТСКИХ СОЦИАЛИСТИЧЕСКИХ РЕСПУБЛИК
ОРДЕНА ЛЕНИНА
МАТЕМАТИЧЕСКИЙ ИНСТИТУТ им. В. А. СТЕКЛОВА
ЛЕНИНГРАДСКОЕ ОТДЕЛЕНИЕ

ЗАПИСКИ НАУЧНЫХ СЕМИНАРОВ ЛОМИ, том 67

ИССЛЕДОВАНИЯ ПО ТЕОРИИ ЧИСЕЛ. 4

Сборник работ под редакцией
А. В. МАЛЫШЕВА

ОТДЕЛЬНЫЙ ОТТИСК

ИЗДАТЕЛЬСТВО «НАУКА»
ЛЕНИНГРАДСКОЕ ОТДЕЛЕНИЕ
Ленинград 1977

Ю.В.Матиясевич

ОДИН КЛАСС КРИТЕРИЕВ ПРОСТОТЫ, ФОРМУЛИРУЕМЫХ В ТЕРМИНАХ ДЕЛИМОСТИ БИНОМИАЛЬНЫХ КОЭФФИЦИЕНТОВ

I. Сравнительно недавно Х.Б.Манн и Д.Шэнкс [I] предложили следующий критерий простоты:

число q является простым тогда и только тогда, когда

$$i \mid \binom{i}{q-2i} \qquad \text{при} \quad i = \left[\frac{q+2}{3}\right], \ldots, \left[\frac{q}{3}\right]$$

(в [I] этот критерий красиво сформулирован в терминах делимости элементов треугольника Паскаля). Они же показали, что их результат является некоторым обобщением теоремы Вильсона.

В отличие от критерия Манна-Шэнкса, в предлагаемых ниже критериях установление простоты сводится к проверке делимости (или неделимости) лишь одного биномиального коэффициента, что, однако, достигается ценой выбора в качестве модуля и аргументов биномиального коэффициента довольно больших чисел. Доказательство основано на одном очень старом, но малоизвестном результате Куммера (см. § 2 в [2], стр.27I в [3] или же [4]; возможно, что работа [2] воспроизведена в [5], однако автор не видел это собрание) о наибольшей степени простого числа, делящей данный биномиальный коэффициент. Эта теорема Куммера позволяет сформулировать много критериев в терминах делимости биномиальных коэффициентов, ниже в качестве примеров приведены три результата такого сорта.

2. Очевидно, что имеет место следующая тривиальная теорема, "сводящая" проверку простоты к делимости одного биномиального коэффициента:

число q является простым тогда и только тогда, когда $2 \mid \binom{2}{f(q)}$, где $f(q)$ - характеристическая функция множества простых чисел.

Интерес к предлагаемым критериям связан с тем, что в них в качестве модуля и аргументов биномиального коэффициента удается брать функции не слишком сложной природы.

Под полиномами всюду ниже понимаются полиномы с целыми коэффициентами. Функцию двух аргументов $F(n,p)$ будем называть экспоненциально-полиномиальной, если $F(n,p) = M(n,p,p^n,\ldots,p^{n^k})$ для некоторого полинома M. Наконец, натуральнозначную функцию $G(n,p)$ будем называть дробно-экспоненциально-полиномиальной, если $G(n,p) = E(n,p) / F(n,p)$, где E, F - экспоненциально-полино-

номиальные функции.

Ниже для общности теоремы сформулированы с двумя параметрами n и p. Чтобы получить именно соответствующие критерии, достаточно явно указать значения этих параметров, например, положить $n=q$, $p=2$.

Теорема А. Можно явно указать полиномы $M'_1,\dots,M'_6$ и натуральнозначные дробно-экспоненциально-полиномиальные функции $B'_1,\dots,B'_6$, $D'_1,\dots,D'_6$ такие, что каковы бы ни были натуральное число n и простое число p, для любого натурального числа q, не превосходящего n, следующие 7 условий эквивалентны:

А0. либо $q=1$, либо q – простое число;

$$A1.\quad p^{M'_1(n)} \mid \binom{B'_1(n,p)}{D'_1(n,p)q};$$

$$A2.\quad p^{M'_2(n)} \nmid \binom{B'_2(n,p)}{D'_2(n,p)q};$$

$$A3.\quad p^{M'_3(n)} \mid \binom{D'_3(n,p)q}{B'_3(n,p)};$$

$$A4.\quad p^{M'_4(n)} \nmid \binom{D'_4(n,p)q}{B'_4(n,p)};$$

$$A5.\quad p^{M'_5(n)} \mid \binom{2(B'_5(n,p)+D'_5(n,p)q)}{B'_5(n,p)+D'_5(n,p)q};$$

$$A6.\quad p^{M'_6(n)} \nmid \binom{2(B'_6(n,p)+D'_6(n,p)q)}{B'_6(n,p)+D'_6(n,p)q}.$$

Ценой небольшого усложнения функций B', D' и M' в условии А0 можно исключить случай $q=1$.

Остается открытым вопрос о возможности такого выбора функ-

ций B', D', M', при котором условие A0 эквивалентно условиям A1*, ..., A6*, получающимся из A1, ..., A6 подстановкой q вместо p.

Теорема B. Можно явно указать полиномы $M''_1, \ldots, M''_6$ и натуральнозначные дробно-экспоненциально-полиномиальные функции $B''_1, \ldots, B''_6$, $D''_1, \ldots, D''_6$ такие, что каковы бы ни были натуральное число n и простое число p, для любого натурального числа q, не превосходящего n, следующие 7 условий эквивалентны:

B0. либо $q=1$, либо q - простое число, либо $q-1$ и $q+1$ - простые числа-близнецы;

B1. $p^{M''_1(n)} \mid \binom{B''_1(n,p)}{D''_1(n,p)q}$;

B2. $p^{M''_2(n)} \nmid \binom{B''_2(n,p)}{D''_2(n,p)q}$;

B3. $p^{M''_3(n)} \mid \binom{D''_3(n,p)q}{B''_3(n,p)}$;

B4. $p^{M''_4(n)} \nmid \binom{D''_4(n,p)q}{B''_4(n,p)}$;

B5. $p^{M''_5(n)} \mid \binom{2(B''_5(n,p)+D''_5(n,p)q)}{B''_5(n,p)+D''_5(n,p)q}$;

B6. $p^{M''_6(n)} \nmid \binom{2(B''_6(n,p)+D''_6(n,p)q}{B''_6(n,p)+D''_6(n,p)}$.

Ясно, что вторая возможность в B0 может реализоваться тогда и только тогда, когда q нечетно или $q=2$, а третья - тогда и только тогда, когда q четно и не равно 2. Случаи $q=1$

и q – простое число также могут быть исключены за счет усложнения функций B'', D'', M''.

Теорема С. Можно явно указать полиномы $M'''_1,\dots,M'''_6$ и натуральнозначные дробно-экспоненциально-полиномиальные функции $B'''_1,\dots,B'''_6$, $D'''_1,\dots,D'''_6$ такие, что каковы бы ни были натуральное число n и простое число p, для любого натурального числа q, не превосходящего n, следующие 7 условий эквивалентны:

С0. либо $q=1$, либо q – простое число Мерсенна, либо $q+1$ – простое число Ферма;,

С1. $$p^{M'''_1(n)} \mid \begin{pmatrix} B'''_1(n,p) \\ D'''_1(n,p)\,q \end{pmatrix};$$

С2. $$p^{M'''_2(n)} \nmid \begin{pmatrix} B'''_2(n,p) \\ D'''_2(n,p)\,q \end{pmatrix};$$

С3. $$p^{M'''_3(n)} \mid \begin{pmatrix} D'''_3(n,p)\,q \\ B'''_3(n,p) \end{pmatrix};$$

С4. $$p^{M'''_4(n)} \nmid \begin{pmatrix} D'''_4(n,p)\,q \\ B'''_4(n,p) \end{pmatrix};$$

С5. $$p^{M'''_5(n)} \mid \begin{pmatrix} 2\,(B'''_5(n,p)+D'''_5(n,p)\,q) \\ B'''_5(n,p)+D'''_5(n,p) \end{pmatrix};$$

С6. $$p^{M'''_6(n)} \nmid \begin{pmatrix} 2\,(B'''_6(n,p)+D'''_6(n,p)\,q) \\ B'''_6(n,p)+D'''_6(n,p)\,q \end{pmatrix}.$$

Упомянутые в теоремах А–С полиномы и дробно-экспоненциально-полиномиальные функции могут быть выбраны многими различными способами; конкретные примеры функций, участвующих в теореме А, приведены в конце статьи.

3. Построение полиномов и дробно-экспоненциально-полиномиальных функций, участвующих в критериях, основано, по-существу,

на том, что множества чисел, удовлетворяющих условиям А0, В0, С0, могут быть определены как множества тех значений параметра q, для которых некоторое диофантово уравнение не имеет решений в целых положительных числах, а именно, для А0 - уравнение

$$q-(x+1)(y+1)=0, \tag{I}$$

для В0 - уравнение

$$\begin{aligned}&[(q-1)-(2x+1)(2y+1)]\times\\ &\times[q-(2x+1)(2y+1)]\times\\ &\times[(q+1)-(2x+1)(2y+1)]=0\end{aligned} \tag{2}$$

для С0 - уравнение

$$\begin{aligned}&[q-(x+1)(2y+1)]\times\\ &\times[(q+1)-(x+1)(2y+1)]=0\end{aligned} \tag{3}$$

При этом важно, что для значений неизвестных можно указать верхнюю оценку в виде степени параметра q (для уравнений (I)-(3) такой оценкой является уже первая степень q). Аналогичные критерии можно дать и для произвольного множества, заданного как множество тех значений параметра, при которых некоторое диофантово уравнение не имеет решения, в котором все значения неизвестных не превосходят значения какого-то полинома от параметра, например, для множества простых чисел вида w^2+1 соответствующим уравнением будет

$$\begin{aligned}&[q-(x+1)(y+1)]\times\\ &\times[((q-((z-1)^2+1))-u)^2+(((z^2+1)-q)-v)^2]=0.\end{aligned} \tag{4}$$

(Уравнения (I)- (3) имеют специальный вид, а именно, входящие в них полиномы представлены в виде произведения линейных по параметру сомножителей. Такой вид действительно необходим для дальнейших преобразований, однако, как заметил Х.Патнам, к этому виду может быть приведено любое уравнение. Действительно, уравнения

$$P(q,z_1,\dots z_k)=0 \tag{5}$$

и

$$q-z_0(1-P(z_0,\dots,z_k))=0 \tag{6}$$

разрешимы при одних и тех же натуральных значениях параметра q.)

Если вместо B, D и M разрешить брать выражения, в которых допускается итерирование возведения в степень, то и в качестве границ для неизвестных можно будет брать функции параметра, получающиеся произвольной композицией сложений, умножений и возведений в степень. Получающийся при этом класс множеств натуральных чисел интересен тем, что он полностью характеризуется наличием критериев рассматриваемого типа – можно показать, что существует диофантово уравнение

$$R(\alpha, \beta, \gamma, z_1, \dots, z_k) = 0 \qquad (7)$$

имеющее решения, не превосходящие

$$(\alpha+\beta+\gamma)^{(\alpha+\beta+\gamma)^{(\alpha+\beta+\gamma)^{(\alpha+\beta+\gamma)^{(\alpha+\beta+\gamma)}}}} \qquad (8)$$

тогда и только тогда, когда

$$\alpha \mid \binom{\beta}{\gamma} \qquad (9)$$

(аналогичное уравнение можно построить и для случая замены (9) на

$$\alpha \nmid \binom{\beta}{\gamma}). \qquad (10)$$

Если мы захотим иметь в качестве границы решений какую-либо еще более быстро растущую функцию φ, то для получения аналогичных критериев надо будет разрешить в построении B, D и M произвольно комбинировать сложение, вычитание, умножение, деление, возведение в степень и функцию φ.

Наконец, если мы отменим вообще ограничения на вид и вычислительный характер функций B, D и M, то критерии рассматриваемого типа можно дать для произвольного множества натуральных чисел.

4. Так же как и критерий Манна-Шэнкса, предлагаемые критерии не имеют вычислительной ценности – это вызвано слишком быстрым ростом участвующих в них функций. Тем не менее, эти критерии могут представить некоторый теоретический интерес, в частности в связи с диофантовыми представлениями простых чисел. Традиционно для построения таких представлений используется теорема

Вильсона. Для случая одноместного предиката " q – простое число" предлагаемые критерии, по-видимому, не дают никаких преимуществ, однако в случае многоместного предиката " $q_1,\dots,q_k$ – простые числа" при большом k и предиката " q – простое число Ферма" эти критерии позволяют строить диофантовы представления с меньшим числом переменных (в случае простых чисел Мерсенна удобнее использовать критерий Люка).

Укажем другую потенциальную область приложения критериев рассматриваемого типа. Согласно известной теореме Лагранжа диофантово уравнение

$$q-((w-1)^2-(x-1)^2-(y-1)^2-(z-1)^2)=0 \qquad (11)$$

разрешимо при любом натуральном q. Используя описанную в настоящей работе технику, можно, исходя из уравнения (11), построить полином M'''' и дробно-экспоненциально-полиномиальные функции B'''' и D'''' такие, что разрешимость (11) эквивалентна условию

$$p^{M''''(n)} \;\Big|\; \binom{B''''(n,p)}{D''''(n,p)q} \qquad (12)$$

где p – простое, $n\geqslant q$. Из теоремы Лагранжа следует, что каково бы ни было простое число p, для любых n и q таких, что $q\leqslant n$, выполнено (12), и, наоборот, если хотя бы при одном простом p условие (12) выполнено для всех n, q таких, что $q\leqslant n$, то любое натуральное является суммой четырех квадратов.

Далее, из (12) следует, что для любого

$$p^{M''''(n)} \;\Big|\; \sum_{q=1}^{n} \binom{B''''(n,p)}{D''''(n,p)q} \qquad (13)$$

Выполнимость (13) для любого n также влечет теорему Лагранжа. Чтобы показать это, достаточно воспользоваться индукцией. Пусть по индукционному предположению числа $1, 2, \dots, q-1$ являются суммами четырех квадратов, тогда по построению B'''', D'''' и M'''' первые $q-1$ слагаемых в сумме (13) делятся на $p^{M''''(n)}$, значит, делится и последнее, и, следовательно, q также есть сумма четырех квадратов.

Функции B'''' и D'''' могут быть построены так, что

$$D''''(n,p)\,n < B''''(n,p) < D''''(n,p)(n+1). \qquad (14)$$

В этом случае правая часть (I3) на единицу меньше левой части формулы

$$\frac{1}{D''''(n,p)} \sum_{i=1}^{D''''(n,p)} (1+\varepsilon_i)^{B''''(n,p)} \equiv 1 \pmod{p^{M''''(n)}}, \qquad (I5)$$

где $\varepsilon_1, \ldots, \varepsilon_{D''''(n,p)}$ – все корни из I степени $D''''(n,p)$. Окончательно получаем, что по теореме Лагранжа для любого простого p имеет место тождественное (по n) сравнение (I5), и, в свою очередь, теорема Лагранжа следует из любого частного случая тождественности сравнения (I5) (то есть достаточно, чтобы (I5) было выполнено для всех n хотя бы при одном простом p).

Рассмотрим теперь постулат Бертрана, для простоты, в виде "для каждого n существует несоставное число q такое, что $[n/2] \le q \le n$". Нам потребуется некоторое усиление теоремы А, а именно, функции B'_2, D'_2 и M'_2 должны удовлетворять следующим дополнительным условиям:

(I). $D'_2(n,p)n < B'_2(n,p) < D'_2(n,p)(n+1)$;

(II). Показатель, с которым p входит в разложение $\binom{B'_2(n,p)}{D'_2(n,p)q}$ кратен n для любого натурального q, не превосходящего n;

(III). Существует полином $\bar{M}(n)$ такой, что

(IIIa). $M'_2(n) > n\bar{M}(n) > 0$;

(IIIb). Свободные коэффициенты M'_2 и $\bar{M}$ равны 0;

(IIIc). Если q – простое число и $q \le n$, то

$$p^{M'_2(n) - [\frac{n-1}{2}]\bar{M}(n)} \Big| \binom{B'_2(n,p)}{D'_2(n,p)q}, \qquad (I6)$$

$$p^{M'_2(n) - [\frac{n+1}{2}]\bar{M}(n)} \Big| \binom{B'_2(n,p)}{D'_2(n,p)q} \qquad (I7)$$

Функции B'_2, D'_2, M'_2 и $\bar{M}$, удовлетворяющие теореме А и этим дополнительным условиям, легко могут быть построены за счет небольшой модификации приведенного ниже доказательства теоремы А.

В терминах рассматриваемых функций постулат Бертрана формулируется следующим образом: для каждого n среди чисел

$$\binom{B_2'(n,p)}{D_2'(n,p)q}, \quad q=\left[\frac{n}{2}\right],\dots,n, \tag{18}$$

есть число, не делящееся на $p^{M_2'(n)}$. Используя вместо A2 более сильное условие (I6), мы можем заменить числа (I8) на кратные им числа

$$\binom{B_2'(n,p)}{D_2'(n,p)q} p^{(n-q)\bar{M}(n)}, \quad q=\left[\frac{n}{2}\right],\dots,n, \tag{19}$$

а затем пополнить этот список числами, которые согласно A2 и (Шс) делятся на $p^{M_2'(n)}$:

$$\binom{B_2'(n,p)}{D_2'(n,p)q} p^{(n-q)\bar{M}(n)}, \quad q=1,\dots,n. \tag{20}$$

Ясно, что если сумма

$$\sum_{q=1}^{n} \binom{B_2'(n,p)}{D_2'(n,p)q} p^{(n-q)\bar{M}(n)+q-1} \tag{21}$$

не делится на $p^{M_2'(n)}$, то какое-то из чисел (20) тоже не делится на $p^{M_2'(n)}$. Менее очевидна справедливость обратного утверждения. Поясним используемую здесь схему рассуждений на более простом примере.

Пусть известно, что число 2 входит в разложения чисел a, b, c с показателем, кратным 3, и

$$2^{12} \mid a+2b+4c. \tag{22}$$

Тогда последовательно заключаем, что $2\mid a$, $2^3\mid a$, $2\mid b$, $2^3\mid b$, $2\mid c$, $2^3\mid c$, $2^4\mid a$, $2^6\mid a$, $2^4\mid b$, $2^6\mid b$, $2^4\mid c$, $2^6\mid c$, $2^7\mid a$ и т.д. до $2^{12}\mid a$, $2^{12}\mid b$, $2^{12}\mid c$.

Таким образом, постулат Бертрана эквивалентен утверждению о том, что для любого n сумма (21) не делится на $p^{M_2'(n)}$.

Следующее преобразование аналогично переходу от (I3) к (I5), и в результате получаем условие

$$\frac{p^{n\bar{M}(n)-1}}{D_2'(n,p)} \sum_{i=1}^{D_2'(n,p)} (1+\lambda_i)^{B_2'(n,p)} \not\equiv 1 \pmod{p^{M_2'(n)}}, \tag{23}$$

где $\lambda_1, \dots, \lambda_{D_2'(n,p)}$ – все корни степени $D_2'(n,p)$ из числа $p^{1-\bar{M}(n)}$. Из постулата Бертрана следует, что (23) выполнено при всех n для любого простого p, и, с другой стороны, из выполнимости (23) для всех n хотя бы при одном простом p следует справедливость постулата Бертрана.

Получаемые на основе описанных критериев переформулировки теоремы Лагранжа и постулата Бертрана отличаются от оригинальных формулировок отсутствием кванторов существования, причем объекты, существование которых утверждается в оригинальных формулировках (разложение на сумму четырех квадратов или простое число в заданных пределах) зависят от n чрезвычайно нерегулярным образом. Представляется интересным развить общие методы исследования поведения по заданному модулю сумм типа входящих в (I5) и (23).

Рассмотрим теперь, какого типа переформулировки можно получать, если вместо условий типа AI – A2 использовать условия типа A3 – A4.

Очевидно, что

$$\frac{(u+1)^{D_3'(n,p)q}}{u^{B_3'(n,p)}} = \sum_{i=B_3'(n,p)}^{D_3'(n,p)q} \binom{D_3'(n,p)q}{i} u^{i-B_3'(n,p)} + \sum_{i=0}^{B_3'(n,p)-1} \binom{D_3'(n,p)q}{i} u^{i-B_3'(n,p)} \tag{24}$$

и, если $u > 2^{D_3'(n,p)n}$, то вторая сумма в (24) меньше I. Следовательно,

$$\left[\frac{(u+1)^{D_3'(n,p)q}}{u^{B_3'(n,p)}}\right] \equiv \binom{D_3'(n,p)q}{B_3'(n,p)} \pmod{u}. \tag{25}$$

Положим

$$u = p^{p^{\ell n^k} F_3'(n,p)}, \tag{26}$$

где ℓ и k столь велики, что

$$p^{\ell n^k} > D_3'(n,p)n, \tag{27}$$

а $F_3'(n,p)$ – знаменатель $B_3'(n,p)$:

$$B'_3(n,p)=\frac{E'_3(n,p)}{F'_3(n,p)}, \qquad (28)$$

где E'_3, F'_3 - положительнозначные экспоненциально-полиномиальные функции.

В результате получаем, что условие А0 эквивалентно условию

$$\left\{H_{n,p}(q)\right\} < p^{-M'_3(n)}, \qquad (29)$$

где фигурные скобки обозначают дробную часть числа, а функция $H_{n,p}$ определена равенством

$$H_{n,p}(q)=\frac{\left(\left(p^{p^{\ell n^k F'_3(n,p)}}+1\right)^{D'_3(n,p)}\right)^q}{p^{p^{\ell n^k E'_3(n,p)}+M'_3(n)}}. \qquad (30)$$

Таким образом, изучение распределения простых чисел сводится к изучению распределения малых дробных частей функции $H_{n,p}$. Трудности использования этого критерия будут связаны, по-видимому, с тем, что функция $H_{n,p}$ "описывает" распределение простых чисел лишь на коротком начальном отрезке $1 \le q \le n$.

Используя А4 вместо А3 можно получить условие, аналогичное (29), но с заменой знака $<$ на $>$.

5. Приведем используемый нами результат Куммера (в терминологии [4]). Пусть $\varkappa_p(t)$ обозначает показатель, с которым простое число p входит в разложение натурального числа t. Пусть, далее, $\tau_p(s,r)$ обозначает число переносов при сложении чисел s и r, записанных в позиционной системе счисления с основанием p.

Теорема (Куммер [2]). Для любого простого числа p и любых натуральных чисел s и r имеет место равенство

$$\varkappa_p\left(\binom{s+r}{s}\right)=\tau_p(s,r). \qquad (31)$$

Доказательство легко получается, например, из равенств

$$\binom{s+r}{s}=\frac{(s+r)!}{s!\,r!}, \qquad (32)$$

$$\varkappa_p(t!)=\left[\frac{t}{p}\right]+\left[\frac{t}{p^2}\right]+\dots. \qquad (33)$$

В дальнейшем вместо функции x_p и биномиальных коэффициентов мы будем работать с функцией τ_p.

В последующих леммах предполагается, что натуральные числа n, p, q, h, l, v, w удовлетворяют неравенствам

$$q < \frac{1}{2} p^{ln}, \quad v \le w < \frac{1}{2} p^{ln}. \tag{34}$$

Лемма I.I. Пусть

$$b_1 = b_1(v, w) = p^{2(h+ln)-1} + w p^{h+ln} - v, \tag{35}$$

$$d_1 = p^{h+ln} - 1. \tag{36}$$

Тогда число $\tau_p(b_1 - d_1 q, d_1 q)$ лежит в интервале $[0, 2ln]$, если $v \le q \le w$, и в интервале $[h, h+2ln]$ в противном случае.

Доказательство. Рассмотрим три случая: $q < v$, $v \le q \le w$, $w < q$. Ниже $\bar{p} = p-1$, а звездочками заменены неизвестные нам цифры в p-ичной записи чисел $b_1 - d_1 q, d_1 q, b_1$. Стрелки $\leftarrow$ указывают наличие переноса из соответствующего разряда, а символ Δ – отсутствие переноса. Цифры 0, 1, $\bar{p}$ отмечены на основе (35), (36) и соответствующих неравенств, связывающих q с v и w. Основанием для знака $\leftarrow$ является либо наличие в соответствующем разряде у обоих слагаемых цифры $\bar{p}$, либо наличие цифры $\bar{p}$ у одного слагаемого и цифры 0 у суммы, причем во втором случае, очевидно, имел место и перенос из предыдущего разряда. Основанием для знака Δ является наличие в соответствующем разряде у одного из слагаемых цифры 0 и совпадение соответствующей цифры второго слагаемого с цифрой суммы, стоящей в том же разряде. Кроме того, знаком Δ отмечен старший разряд суммы, из которого заведомо нет переноса. Неравенства (34) гарантируют нам, что запись чисел $q, v, w, |q-v|, |q-w|$ имеет длину не более ln. Требуемые неравенства получаются простым подсчетом знаков $\leftarrow$ и Δ.

Случай $q < v$.

$$\begin{array}{rl}
 & \overbrace{}^{h-1}\ \overbrace{}^{ln}\ \overbrace{}^{h}\ \overbrace{}^{ln} \\
b_1 - d_1 q = & 1\,\underbrace{0\ldots0}\ \underbrace{*\ldots*}\ \underbrace{\bar{p}\ldots\bar{p}}\ \underbrace{*\ldots*} \\
d_1 q = & \qquad\quad\ \underbrace{*\ldots*}\ \underbrace{\bar{p}\ldots\bar{p}}\ \underbrace{*\ldots*} \\
\hline
b_1 = & 1\,0\ldots0\ *\ldots*\ \bar{p}\ldots\bar{p}\ *\ldots* \\
 & \Delta\ \Delta\ldots\Delta \qquad\quad \leftarrow\ldots\leftarrow
\end{array}.$$

Случай $v \le q \le w$.

$$
\begin{array}{lll}
b_1 - d_1 q = 1 \overbrace{0\ldots0}^{h-1} \overbrace{*\ldots*}^{\ell n} \overbrace{0\ldots0}^{h} \overbrace{*\ldots*}^{\ell n} \\
d_1 q = \qquad\quad *\ldots* \quad \bar{p}\ldots\bar{p} \quad *\ldots* \\
\hline
b_1 = 1\,0\ldots0 \quad *\ldots* \quad \bar{p}\ldots\bar{p} \quad *\ldots* \\
\qquad\quad \Delta\,\Delta\ldots\Delta \qquad\quad \Delta\ldots\Delta
\end{array}
$$

Случай $w < q$.

$$
\begin{array}{lll}
b_1 - d_1 q = \overbrace{\bar{p}\ldots\bar{p}}^{h-1} \overbrace{*\ldots*}^{\ell n} \overbrace{0\ldots0}^{h} \overbrace{*\ldots*}^{\ell n} \\
d_1 q = \qquad\quad *\ldots* \quad \bar{p}\ldots\bar{p} \quad *\ldots* \\
\hline
b_1 = 1\,0\ldots0 \quad *\ldots* \quad \bar{p}\ldots\bar{p} \quad *\ldots* \\
\qquad\quad \leftarrow\ldots\leftarrow \quad \leftarrow \qquad\quad \Delta\ldots\Delta
\end{array}
$$

Лемма доказана.

Следующие пять лемм доказываются аналогично лемме I.I.

Лемма I.2. Пусть

$$b_2 = b_2(v, w) = p^{2(h+\ell n)-1} + v p^{h+\ell n} - (w+1), \tag{37}$$

$$d_2 = p^{h+\ell n} - 1. \tag{38}$$

Тогда число $\tau_p(b_2 - d_2 q, d_2 q)$ лежит в интервале $[2h, 2h+2\ell n]$, если $v \le q \le w$, и в интервале $[h, h+2\ell n]$ в противном случае.

Лемма I.3. Пусть

$$b_3 = b_3(v, w) = v p^{h+\ell n} - w, \tag{39}$$

$$d_3 = p^{3(h+\ell n)} - p^{2(h+\ell n)} + p^{h+\ell n} - 1. \tag{40}$$

Тогда число $\tau_p(d_3 q - b_3, b_3)$ лежит в интервале $[0, 4\ell n]$, если $v \le q \le w$, и в интервале $[h, h+4\ell n]$ в противном случае.

Лемма I.4. Пусть

$$b_4 = b_4(v,w) = 2wp^{h+\ell n} - (2v-1), \tag{41}$$

$$d_4 = 2p^{3(h+\ell n)} - 2p^{2(h+\ell n)} + 2p^{h+\ell n} - 2. \tag{42}$$

Тогда число $\tau_p(d_4q - b_4, b_4)$ лежит в интервале $[2h, 2h+4\ell n]$, если $v \le q \le w$, и в интервале $[h, h+4\ell n]$ в противном случае.

Лемма I.5. Пусть

$$b_5 = b_5(v,w) = p^{2(h+\ell n)-1} - vp^{h+\ell n} + w, \tag{43}$$

$$d_5 = p^{h+\ell n} - 1. \tag{44}$$

Тогда число $\tau_p(b_5 + d_5 q, b_5 + d_5 q)$ лежит в интервале $[0, 2\ell n]$, если $v \le q \le w$, и в интервале $[h, h+2\ell n]$ в противном случае.

Лемма I.6. Пусть

$$b_6 = b_6(v,w) = p^{2(h+\ell n)-1} - wp^{h+\ell n} + (v-1), \tag{45}$$

$$d_6 = p^{h+\ell n} - 1. \tag{46}$$

Тогда число $\tau_6(b_6 + d_6 q, b_6 + d_6 q)$ лежит в интервале $[2h, 2h+2\ell n]$, если $v \le q \le w$, и в интервале $[h, h+2\ell n]$ в противном случае.

Лемма 2. Пусть p, x, y, v, w, k - натуральные числа, удовлетворяющие неравенству $x + y < p^k$. Тогда

$$\tau_p(vp^k + x, wp^k + y) = \tau_p(v,w) + \tau_p(x,y).$$

Доказательство очевидно.

Лемма 3.I. Пусть d - натуральное число, $v_1, \dots, v_s$ - произвольный список (быть может, с повторениями) натуральных чисел, удовлетворяющих неравенствам

$$v_i + d < \frac{1}{2} p^{\ell n} \tag{47}$$

Положим

$$B_1 = \sum_{i=1}^{s} b_1(v_i, v_i+d-1)\, p^{2(h+ln)(i-1)}, \tag{48}$$

$$D_1 = \sum_{i=1}^{s} d_1 p^{2(h+ln)(i-1)}. \tag{49}$$

Тогда, если одно из чисел $q, q+1, \dots, q+d-1$ совпадает с одним из чисел $v_1, \dots, v_s$, то

$$\tau_p(B_1 - D_1 q, D_1 q) \leq (s-1)h + 2sln, \tag{50}$$

в противном случае

$$\tau_p(B_1 - D_1 q, D_1 q) \geq sh. \tag{51}$$

Лемма непосредственно следует из лемм I.I и 2. Аналогично можно сформулировать и доказать еще пять лемм 3.2-3.6.

Для завершения доказательства теорем A, B и C выберем число h столь большим, что

$$h > 4sln. \tag{52}$$

Теперь мы можем найти целые числа $m_1, \dots, m_6$ такие, что

$$(s-1)h + 2sln < m_1 \leq sh, \tag{53}$$

$$sh + 2sln < m_2 \leq (s+1)h, \tag{54}$$

$$(s-1)h + 4sln < m_3 \leq sh, \tag{55}$$

$$sh + 4sln < m_4 \leq (s+1)h, \tag{56}$$

$$(s-1)h + 2sln < m_5 \leq sh, \tag{57}$$

$$sh + 2sln < m_6 \leq (s+1)h. \tag{58}$$

Для получения теоремы A согласно (I) можно положить $d=1$, $s=n^2$, $v_{(x-1)n+y} = (x+1)(y+1)$ $(x,y=1,\dots,n)$, $l=4$, $h=16n^3-4n$. Аналогично в случае теоремы B согласно (2) полагаем $d=3$, $s=n^2$, $v_{(x-1)n+y} = (2x+1)(2y+1)$ $(x,y=1,\dots,n)$, $l=5$, $h=20n^3-5n$. Наконец, для теоремы C согласно (3) полагаем $d=2$, $s=n^2$, $v_{(x-1)n+y} = (x+1)(2y+1)$ $(x,y=1,\dots,n)$, $l=5$, $h=20n^3-5n$. Требуемые дробно-экспоненциально-полиномиальные функции получаются теперь по стандартным формулам суммирования:

$$\sum_{i=0}^{k} t^i = \frac{t^{k+1}-1}{t-1}, \qquad (59)$$

$$\sum_{i=0}^{k} i t^i = \frac{k t^{k+2} - (k+1)t^{k+1} + t}{(t-1)^2}. \qquad (60)$$

Приведем окончательные выражения для всех функций, участвующих в теореме А.

Пусть

$$T = (p^{32n^5}-1)(p^{32n^3}-1)^{-1},$$

$$R = \{(n^2+2n+1)p^{32n^5+64n^4+32n^3} -$$

$$-(n^2+3n+2)p^{32n^5+64n^4} - (n^2+4n+3)p^{32n^5+32n^4+32n^3} +$$

$$+(n^2+6n+6)p^{32n^5+32n^4} + (n+2)p^{32n^5+32n^3} -$$

$$-(2n+4)p^{32n^5} - (n+1)p^{64n^4+32n^3} -$$

$$-(n+2)p^{64n^4} + (2n+3)p^{32n^4+32n^3} - (2n+6)p^{32n^4} -$$

$$-2p^{32n^3} + 4\} \times$$

$$\times (p^{16n^3}-1)^{-1}(p^{16n^3}+1)^{-2}(p^{32n^4}-1)^{-2}.$$

Тогда можно положить

$$B_1' = p^{32n^3-1}T + R,$$
$$B_2' = (p^{32n^3-1}-1)T + R,$$
$$B_3' = R,$$
$$B_4' = T + 2R,$$
$$B_5' = p^{32n^3-1}T - R,$$
$$B_6' = (p^{32n^3-1}-1)T - R,$$

$$D_1' = D_2' = (p^{32n^5}-1)(p^{16n^3}+1)^{-1},$$

$$D_3' = (p^{64n^5}-1)(p^{32n^3}+1)^{-1},$$

$$D_4' = 2D_3',$$

$$D_5' = D_6' = D_1',$$

$$M_1' = 16n^5 - 4n^3,$$

$$M_2' = 16n^5 + 12n^3 - 4n,$$

$$M_3' = M_1',$$

$$M_4' = M_2',$$

$$M_5' = M_1',$$

$$M_6' = M_2'.$$

Литература.

1. Mann H.B., Shanks D. .A necessary and sufficient condition for primality and its source.-J.Combinatorical Theory, Ser.A, 1972, 13, p.131-134.
2. Kummer E.E. Uber die ergänzungssatre zu den algemeinen Reciprocitätsgesetren.-J.reine und angew. Math., 1852, 44, S.93-146.
3. Dickson L.E. History of the theory of numbers. Vol. I. Divisibility and primality. Chelsea Publ.Co., New York, 1952.
4. Singmaster D. Notes on binomial coefficients I. A generaliration of Lucas congruence.-J.London Math.Soc., 1974, 8, № 3, p.545-548.
5. Ernst Eduard Kummer collected papers. Vol.I. Contributions to number theory. Ed. A.Weil. Berlin a.o., Springer, 1975, VIII, 957 p.