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

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

(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 $2 \,\Big|\, \binom{2}{f(q)}$, 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-