УДК 511.2(075.8)

К.Ф. Филозоф

ОДИН СПОСОБ ВЫЧЛЕНЕНИЯ ПРОСТЫХ ЧИСЕЛ

В работе рассмотрен способ отыскания простых чисел на отрезках натурального ряда, базирующийся на методе «решета» Эратосфена. Множество чисел рассматриваемого отрезка разбивается на подмножества (арифметические прогрессии), содержащиеся в классах вычетов по некоторому модулю m. Обоснован оптимальный вариант выбора модуля m для $2 \le m \le 200$, позволяющий исследовать на простоту минимально достаточное количество чисел выбранного отрезка. Эффективность предложенного способа проиллюстрирована примерами.

Введение

Множество натуральных чисел является базовым для построения различных математических теорий, в конечном итоге – для всей математики. Исследование натуральных чисел ведется с древних времен. Уже в IV-м веке до н. э в пифагорейской школе были получены важные результаты, имеющие фундаментальное значение для этой отрасли математической науки, получившей название «теоретическая арифметика», или более современное «теория чисел». В частности, были заложены основы теории делимости в кольце целых чисел, выделены простые и составные числа, выявлены их основные свойства. Число называется простым, если оно имеет всего два натуральных делителя, и составным, если у него имеется больше двух натуральных делителей. Число «один», таким образом, не относится ни к простым, ни к составным. Каждое составное число может быть записано в виде произведения простых чисел, и это представление единственно, если не учитывать порядок записи множителей (основная теорема арифметики). Представление натурального числа n, отличного от единицы, в виде $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, где p_i – различные простые числа, а α_i – натуральные числа, $i = \overline{1,k}$, называется каноническим разложением числа n на простые множители. Отсюда видно, какую важную роль играют простые числа, являясь, по сути, «кирпичиками» всего здания математической науки. Уже древнегреческим математикам был известен критерий простого числа: число a будет простым тогда и только тогда, когда оно не делится ни на одно простое число, не превосходящее $\sqrt{a}$. В III-м веке до н.э. в своих знаменитых «Началах» Эвклид изложил систематическое построение теории делимости, привел алгоритм нахождения наибольшего общего делителя (НОД) двух чисел, доказал, что множество простых чисел бесконечно. Эратосфен (276–196 гг. до н.э.) предложил способ отыскания простых чисел, не превышающих данного натурального числа a («решето» Эратосфена). Он состоит в том, что из данного множества вычеркивают все числа, делящиеся на простые числа p, где $p \le \sqrt{a}$, кроме самих этих простых чисел. Причем для выяснения того, делится ли данное число на простое число p, необязательно знать признаки делимости или выполнять непосредственное деление на p. Ведь на p делится каждое p-е число в натуральном ряду после любого числа, делящегося на p. Вычеркивая таким образом все числа, начиная с $2p$ (и даже с p^2), для всех простых $p \le \sqrt{a}$, включая и вычеркнутые ранее, получим на отрезке $[1;a]$ невычеркнутыми только все простые числа и число 1. В настоящее время составлены таблицы про-

стых чисел до 15000000 (разумеется, не «вручную»). Расцвет теории чисел начался в VII–VIII вв. (труды Ферма, Паскаля, Декарта, Эйлера, Гаусса). И еще более значительные успехи в теоретико-числовых исследованиях были достигнуты в XIX–XX вв., когда были открыты новые, революционные по своей сущности методы и получены принципиально новые результаты (Дедекинд, Риман, Коши, Дирихле, Чебышев, Чеботарев, Шнирельман, Виноградов, Хинчин, Линник и др.). Интерес к теоретико-числовым проблемам, задачам не ослабевает и сейчас.

Относительно рассматриваемой в нашей работе темы отметим следующее: 1) очень много задач на простые и составные числа, имеющих, казалось бы, простую формулировку, не решены до сих пор; 2) даже решенные задачи, проблемы могут дать много полезного для развития математического мышления тех, кто изъявит желание найти свой способ их решения. Этот второй аспект мы считаем тоже важным, можно даже сказать, прикладным аспектом математической науки. Именно он явился мотивационным для выбора темы нашей работы, ее основной целью; 3) тематика статьи входит в вузовский курс алгебры и теории чисел, являющийся базовым в подготовке бакалавра по специальности «математика». Предложенная нами работа может оказаться интересной студентам при изучении этого предмета. Изложение темы не предполагает углубленных познаний в теории чисел, поэтому доступно не только студентам, но и ученикам старших классов средней школы, занимающихся в математических кружках или изучающих математику глубже на факультативных занятиях. Поэтому мы приводим достаточно детализированные выкладки, многие из которых очевидны для специалистов. Учителю несложно будет предварительно адаптировать ДЛЯ учеников неизвестные им математические понятия и факты, имеющиеся в работе.

И если после ознакомления с нашей работой у кого-то возникнет интерес к затронутым в ней вопросам, желание углубить свои познания о простых числах, мы будем считать свою цель достигнутой.

Постановка задачи, обоснование способа решения

Решим задачу: выделить все простые числа, не превышающие некоторого натурального числа a.

Как было отмечено выше, задачу можно решить с помощью классического «решета» Эратосфена. Но при больших значениях a приходится исследовать огромное количество чисел. Это, понятно, громоздкий процесс.

Зададимся целью найти оптимальный способ решения нашей задачи, то есть сократить до определенного минимума количество проверяемых на простоту чисел, не упустив ни одного простого числа.

При этом используем следующие свойства простых и составных чисел:

- каждое число или делится на простое число, или взаимно простое с ним;
- каждое составное число имеет по крайней мере один простой делитель;
- минимальный простой делитель составного числа a не превышает $\sqrt{a}$, а также упомянутый во вступлении критерий простого числа, являющийся следствием этих свойств.

Сократить количество проверяемых чисел можно, например, так: отбросить все четные, кроме числа 2, являющегося единственным простым четным. Тогда для проверки останется половина от начального количества чисел. Но и половина – это еще много. Рассмотрим теперь любое натуральное число m, допустим, в пределах $2 < m \le 50$ и выделим из нашего множества отдельные подмножества чисел, имеющие

при делении на m одинаковые остатки. Такие числа называются конгруэнтными по модулю m, а классы конгруэнтных по модулю m чисел называются классами вычетов по модулю m. Факт конгруэнтности чисел a и b по модулю m записывают так: $a \equiv b(\mathrm{mod}\, m)$. В зависимости от остатка при делении чисел одного класса вычетов на модуль m можно все такие классы обозначить символами: $K_0^{(m)}$, $K_1^{(m)}$, $K_2^{(m)}$, …, $K_{m-1}^{(m)}$. Их объединение составляет множество Z всех целых чисел. Но символы внизу не обязательно должны быть остатками от деления чисел из этого класса на m, сюда можно поставить любое число из данного класса. Итак, $K_r^{(m)} = \{x : x \equiv r(\mathrm{mod}\, m)\} = \{r + mt, t \in Z\}$. Легко доказывается теорема о том, что все числа из одного класса вычетов по модулю m имеют с модулем m один и тот же НОД, то есть если $a \in K_r^{(m)}$, то $(a,m) = (r,m)$. Из этого следует, что если хоть одно число из класса $K_r^{(m)}$ будет взаимно простым с модулем, то и все числа из этого класса будут взаимно просты с модулем (говорят еще: весь класс взаимно прост с модулем).

Если для решения поставленной нами задачи разбить множество данных натуральных чисел из отрезка $[1;a]$ на подмножества, содержащиеся, например, в классах вычетов по модулю 7, то получим, что класс $K_0^{(7)}$ состоит из составных чисел, делящихся на 7, за исключением самого числа 7, являющегося простым. Значит, этот класс можно и не рассматривать, выписав лишь из него само число 7. Но остальные шесть классов по модулю 7 содержат в себе как простые, так и составные числа. Следовательно, эти классы, содержащие $\frac{6}{7}$ от всего количества чисел, подлежат исследованию. Получили еще хуже результат, чем при распределении на четные и нечетные числа. То есть при выборе $m = 2$ чисел для проверки остается намного меньше, чем при выборе $m = 7$.

Разобьем теперь наш отрезок по классам вычетов по модулю 30. Получаем совсем другую картину: на нашем отрезке в классах $K_2^{(30)}$, $K_3^{(30)}$, $K_5^{(30)}$ будет всего по одному простому числу 2, 3 и 5 соответственно, все остальные числа в них составные, кратные указанным простым. Далее, во всех других классах $K_r^{(30)}$, где $(r,30) > 1$, простых чисел быть не может. Действительно, любое число n, принадлежащее классу $K_r^{(30)}$ в рассматриваемом нами множестве $[1;a]$, имеет вид $n = r + 30k$, $k \in \mathrm{N}$, причем $(n,30) = (r,30) > 1$. И тогда n делится хотя бы на один простой делитель числа 30, не совпадая с этим простым делителем. Значит, оно составное. Итак, все такие классы можно не рассматривать. Для исследования остаются только классы, взаимно простые с модулем. Их количество равно $\varphi(30) = 8$ (по определению функции Эйлера), остальные 22 класса не рассматриваем, ибо в них нет простых чисел, за исключением трех отмеченных ранее чисел 2, 3 и 5. Например, если взять $a = 600$, то эти 600 чисел мы распределим в зависимости от остатков при делении на 30 в 30 классов по 20 чисел в каждом, а для проверки останется лишь 160 чисел, то есть меньше трети чисел, имеющихся вначале.

Приведенные примеры позволяют сделать некоторые предварительные выводы.

Во-первых, если распределить числа в классы вычетов по модулю m, то для проверки следует оставить только $\varphi(m)$ классов, взаимно простых с модулем, в других классах нет простых чисел, за исключением простых делителей модуля, которые можно записать с самого начала.

Во-вторых, не стоит брать простой модуль p, так как $\varphi(p)=p-1$, и слишком много чисел остается для проверки.

В-третьих, очевидно, что в случае, если $\varphi(m_1)=\varphi(m_2)$, а $m_1>m_2$, что тоже не исключено, более эффективным будет модуль m_1, то есть больший из этих модулей, поскольку классов для проверки остается одинаковое количество, но в классах по большему модулю содержится меньше чисел.

В-четвертых, очевидно, что эффективность модуля определяется отношением $\frac{\varphi(m)}{m}$: чем оно меньше, тем лучше подходит число m в роли модуля для распределения имеющихся чисел по классам вычетов по данному модулю, состоящих из чисел вида $mk+r$, где $(r,m)=1$. Этот вывод является главным для решения нашей задачи.

Мы исследовали все числа m, не превосходящие числа 200. Простые числа p сразу отбрасываем, поскольку отношение $\frac{\varphi(p)}{p}=\frac{p-1}{p}$ слишком близко к единице.

В таблице 1 приведены результаты для составных m, где $10\le m\le 50$.

Таблица 1

m	$\varphi(m)$	$\frac{\varphi(m)}{m}$	m	$\varphi(m)$	$\frac{\varphi(m)}{m}$	m	$\varphi(m)$	$\frac{\varphi(m)}{m}$
10	4	0,4	25	20	0,8	38	18	0,473…
12	4	0,(3)	26	12	0,461…	39	24	0,615…
14	6	0,428…	27	18	0,(6)	40	16	0,4
15	8	0,533…	28	12	0,428…	**42**	**12**	**0,285…**
16	8	0,5	***30***	***8***	***0,2(6)***	44	20	0,454…
18	6	0,(3)	32	16	0,5	45	24	0,533…
20	8	0,4	33	20	0,606…	46	22	0,478…
21	12	0,571…	34	16	0,470…	48	16	0,(3)
22	10	0,454…	35	24	0,685…	49	42	0,875…
24	8	0,(3)	36	12	0,(3)	50	20	0,4

Таблица показала, что минимальное отношение $\frac{\varphi(m)}{m}$ будет при единственном $m=30$: $\frac{\varphi(30)}{30}=0,2(6)$. Незначительно отличается результат для $m=42$: $\frac{\varphi(42)}{42}=0,285...$. Все остальные отношения больше этих двух.

Рассмотрев все остальные m, не превышающие числа 200, мы получили следующие результаты:

$$\frac{\varphi(60)}{60}=\frac{\varphi(90)}{90}=\frac{\varphi(120)}{120}=\frac{\varphi(150)}{150}=\frac{\varphi(180)}{180}=\frac{\varphi(30)}{30}=0,2(6).$$

$$\frac{\varphi(84)}{84}=\frac{\varphi(126)}{126}=\frac{\varphi(168)}{168}=\frac{\varphi(42)}{42}=0,(285714).$$

Укажем также, для каких еще чисел m рассматриваемое отношение незначи-

тельно отличается от минимального и является меньшим, чем одна треть.

$\frac{\varphi(66)}{66}=\frac{\varphi(132)}{132}=\frac{\varphi(198)}{198}=0,(30);$ $\frac{\varphi(78)}{78}=\frac{\varphi(156)}{156}=0,(307692);$

$\frac{\varphi(102)}{102}=0,313\ldots;$ $\frac{\varphi(114)}{114}=0,315\ldots;$ $\frac{\varphi(138)}{138}=0,318\ldots;$ $\frac{\varphi(186)}{186}=0,322\ldots$.

Для всех остальных значений модуля интересующее нас отношение является не меньшим одной трети.

Итак, мы нашли оптимальный модуль $m=30$ (либо 60, 90, 120, 150, 180). Остановим свой выбор на $m=30$. Тогда исследуемые числа распределяем по таким классам, взаимно простым с 30: $K_1^{(30)}$, $K_7^{(30)}$, $K_{11}^{(30)}$, $K_{13}^{(30)}$, $K_{17}^{(30)}$, $K_{19}^{(30)}$, $K_{23}^{(30)}$, $K_{29}^{(30)}$. Условимся числа одного класса записывать в столбик (хотя это не обязательно, можно и по строчкам). Запись чисел в каждом столбике очень легка: каждое последующее число получаем из предыдущего прибавлением числа 30 (модуля), это следует из определения конгруэнтных чисел. Значит, все числа в каждом классе представляют собой арифметическую прогрессию с разностью, равной выбранному модулю. Более того, при наших оптимальных модулях все члены прогрессии даже оканчиваются на одну и ту же цифру, что очень удобно для записи чисел в таблицу. Количество столбиков равняется $\varphi(m)$, для $m=30$ их число равно 8, для $m=60$ их будет $\varphi(60)=16$ и т.д. Количество строчек зависит от данного в условии числа a.

Как было установлено, минимально достаточное количество чисел, подлежащих рассмотрению на простоту, для модулей 30, 60, 90, 120, 150, 180 одинаково. Но может возникнуть вопрос: будут ли все исследуемые числа при этих разных модулях тоже одними и теми же? Не случится ли так, что при одном из этих модулей какое-то число подлежит исследованию, а при другом модуле оно выпадет из поля зрения? Ответ получим, исходя из канонического разложения этих модулей.

$30=2\cdot3\cdot5;$ $60=2^2\cdot3\cdot5;$ $90=2\cdot3^2\cdot5;$

$120=2^3\cdot3\cdot5;$ $150=2\cdot3\cdot5^2;$ $180=2^2\cdot3^2\cdot5.$

Видим, что все числа имеют одни и те же простые делители. В нашей таблице мы записываем только те числа, которые взаимно просты с модулем. Обратимся теперь к следующему свойству взаимно простых чисел: число n будет взаимно простым с числом m, если n не делится ни на один простой делитель числа m. Отсюда вывод: представленные в таблицах, составленных по указанным модулям, множества чисел, взаимно простых с каждым из этих модулей, полностью совпадают.

Чтобы получить при помощи «решета» Эратосфена все простые числа в так составленной таблице, надо в каждом столбике вычеркнуть каждое число, делящееся на простое p, кроме самого p, для всех $p\le\sqrt{a}$ (напомним, что a – максимальное число таблицы). Покажем, что и в нашей таблице принцип вычеркивания остается таким же, как и в классическом «решете» Эратосфена: на 7 делится каждое седьмое после найденного любого в столбике, делящегося на 7; на 11 – каждое одиннадцатое и т.д.

Действительно, в каждом столбике $K_r^{(30)}$ каждое $x_k\in K_r^{(30)}$ имеет вид $x_k=r+30k$, $k\in\mathrm{N}$, а седьмым после него в столбике является $x_{k+7}=r+30(k+7)$, $k\in\mathrm{N}$, то есть $x_{k+7}=x_k+30\cdot7$. Если $x_k\vdots7$, то получится, что и $x_{k+7}\vdots7$, причем между ними чисел, делящихся на 7, нет, так как число $x_{k+s}=x_k+30\cdot s$ при $1<s<7$ на 7 не делится. Аналогично будет для всех остальных простых чисел и, соответственно, моду-

лей. Поэтому будет легко вычеркивать соответствующие составные числа в таблице, отыскав любое из них (чаще всего первое в столбике). На том, как находить это первое число в нетривиальных случаях, мы остановимся ниже, рассматривая примеры. После выполнения процедуры вычеркивания для всех простых $p \le \sqrt{a}$ в таблице останутся только простые числа, кроме простых делителей модуля, и число 1. Таким образом будут найдены все простые числа, не превышающие числа a. Задача решена.

Примеры

Пример 1. Составить таблицу простых чисел, не превышающих числа 600.

Решение. Как было установлено, все натуральные числа, не превышающие числа 600, можно распределить по классам вычетов по модулю 30 (или по модулям, равноценным этому с точки зрения оптимальности решения). Поэтому для проверки останутся всего 160 чисел из 600. Они будут записаны в 8 столбиках и 20 строчках. В таблице 2 мы выписали только первые и последние три строки.

Таблица 2

$K_1^{(30)}$	$K_7^{(30)}$	$K_{11}^{(30)}$	$K_{13}^{(30)}$	$K_{17}^{(30)}$	$K_{19}^{(30)}$	$K_{23}^{(30)}$	$K_{29}^{(30)}$
1	7	11	13	17	19	23	29
31	37	41	43	47	49	53	59
61	67	71	73	77	79	83	89
…	…	…	…	…	…	…	…
511	517	521	523	527	529	533	539
541	547	551	553	557	559	563	569
571	577	581	583	587	589	593	599

Далее: $\sqrt{600} \approx 25$.

Выписываем все простые числа, не превышающие 25, начиная с 7: 7, 11, 13, 17, 19, 23, 29. Затем вычеркнем согласно описанному выше алгоритму все составные числа, делящиеся на эти простые. К оставшимся невычеркнутыми числам, кроме числа 1, не забудем добавить простые делители числа 30, о которых сказано вначале, и тогда получаем все простые числа, не превышающие числа 600. Мы их записали в таблице 3.

Таблица 3

2	31	73	127	179	233	283	353	419	467	547
3	37	79	131	181	239	293	359	421	479	557
5	41	83	137	191	241	307	367	431	487	563
7	43	89	139	193	251	311	373	433	491	569
11	47	97	149	197	257	313	379	439	499	571
13	53	101	151	199	263	317	383	443	503	577
17	59	103	157	211	269	331	389	449	509	587
19	61	107	163	223	271	337	397	457	521	593
23	67	109	167	227	277	347	401	461	523	599
29	71	113	173	229	281	349	409	463	541	

В следующем примере мы рассмотрим более удаленные от начала отрезки натурального ряда и найдем на них все простые числа.

Пример 2. Найти все простые числа на отрезке $[5201;5534]$.

Решение. На этом отрезке есть 334 натуральных числа. Как и в предыдущем примере, распределим их по классам вычетов по модулю 30, и тогда останется для проверки только 90 чисел (таблица 4). Выписываем все простые числа $p \le \sqrt{5534} \approx 75$, кроме 2, 3, 5 (как было сказано выше, в таблице нет чисел, кратных этим простым числам): 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73. Для каждого такого простого p находим в каждом столбике первое число, делящееся на p, вычеркиваем его и каждое p-е после него. Например, для $p = 7$ будут вычеркнуты числа (по столбикам): 5341; 5257 и 5467; 5383; 5327; 5299 и 5509; 5243 и 5453; 5369.

Таблица 4

$K_1^{(30)}$	$K_7^{(30)}$	$K_{11}^{(30)}$	$K_{13}^{(30)}$	$K_{17}^{(30)}$	$K_{19}^{(30)}$	$K_{23}^{(30)}$	$K_{29}^{(30)}$
		5201	5203	5207	**5209**	5213	5219
5221	**5227**	**5231**	**5233**	**5237**	5239	5243	5249
5251	5257	**5261**	**5263**	5267	5269	**5273**	**5279**
5281	5287	5291	5293	**5297**	5299	**5303**	**5309**
5311	5317	5321	**5323**	5327	5329	**5333**	5339
5341	**5347**	**5351**	5353	5357	5359	**5363**	5369
5371	5377	**5381**	5383	5387	5389	**5393**	**5399**
5401	**5407**	5411	**5413**	**5417**	**5419**	5423	5429
5431	**5437**	**5441**	**5443**	5447	**5449**	5453	5459
5461	5467	**5471**	5473	**5477**	**5479**	**5483**	5489
5491	5497	**5501**	**5503**	**5507**	5509	5513	**5519**
5521	**5527**	**5531**	5533				

После выполнения всех вычеркиваний в таблице получим невычеркнутыми 42 числа, это и есть все искомые простые числа на отрезке $[5201;5534]$. Здесь они выделены жирным шрифтом. Из них 8 пар так называемых чисел- «близнецов», то есть простых чисел, разность между которыми равна 2. В таблице они подчеркнуты.

Замечание 1. Чтобы упростить поиск чисел, делящихся на p, можно поступить следующим образом: найти минимальное и максимальное значение $q_{\min}$ и $q_{\max}$ частного от деления на p чисел этой таблицы, потом для $q \in [q_{\min}; q_{\max}]$ найти произведения qp, являющиеся искомыми составными числами, делящимися на p. Еще отметим, что из всех таких q можно сразу отбросить делящиеся либо на 2, либо на 3, либо на 5, поскольку заведомо известно, что чисел вида $2t$, $3t$, $5t$ ($t \in \mathrm{N}$) в таблице нет. Например, для $p = 43$ получаем $\frac{5201}{43} = 120{,}9...$; $\frac{5533}{43} = 128{,}6...$; таким образом, $q_{\min}(43) = 121$ и $q_{\max}(43) = 128$. Из этих $q \in [120;128]$ отсеиваем кратные 2, 3, 5, после чего остаются всего два значения: $q = 121$ и $q = 127$. Получили, что в нашей таблице есть только два числа, делящихся на 43: $121 \cdot 43 = 5203$ и $127 \cdot 43 = 5461$. Для $p = 47$ получаем

$\frac{5201}{47}=110{,}6...$; $\frac{5533}{47}=117{,}7...$; то есть $q_{\min}(47)=111$ и $q_{\max}(47)=117$. Из этих $q\in[111;117]$ отсеиваем кратные 2, 3, 5, после чего остается всего одно значение $q=113$. Получили, что в нашей таблице есть только одно число, делящееся на 43: $113\cdot 47=5311$. Кстати, для многих простых p здесь будет всего одно или два числа, кратных p, поэтому процесс вычеркивания будет не особо громоздким.

Если таблица довольно большая, то отыскать в каждом столбике $K_r^{(m)}$ первое (как и любое) число, делящееся на данное простое p, можно при помощи конгруэнций. Если $x\vdots p$, то $x\equiv 0(\mathrm{mod}\,p)$, или $r+mt\equiv 0(\mathrm{mod}\,p)$. Допустимые значения параметра t получим из неравенств $a\le x\le b$, где a и b – минимальное и максимальное числа в этом столбике. Можно ограничиться лишь одним неравенством $x\ge a$, если искать только первое число столбика, делящееся на p. Найдем таким способом, например, числа в первом столбике таблицы 4, делящиеся на 13 и на 17. Для этого решаем две конгруэнции: $1+30t\equiv 0(\mathrm{mod}13)$ и $1+30k\equiv 0(\mathrm{mod}17)$, $t,k\in\mathrm{N}$. Обозначим $x=1+30t$ и $y=1+30k$.

$1+30t\equiv 0(\mathrm{mod}13)$;	$1+30k\equiv 0(\mathrm{mod}17)$;
$30t\equiv -1(\mathrm{mod}13)$;	$30k\equiv -1(\mathrm{mod}17)$;
$4t\equiv 12(\mathrm{mod}13)$;	$-4k\equiv 16(\mathrm{mod}17)$;
$t\equiv 3(\mathrm{mod}13)$;	$k\equiv -4(\mathrm{mod}17)$;
$t=3+13m$; $m\in\mathrm{N}$;	$k=-4+17s$; $s\in\mathrm{N}$;
$x=1+30\cdot(3+13m)=91+390m$.	$y=1+30\cdot(-4+17s)=-119+510s$.

Допустимые значения параметров находим из неравенств $5221\le x\le 5521$, $5221\le y\le 5521$. Получим: $13\frac{2}{13}\le m\le 13\frac{12}{13}$; $10\frac{8}{17}\le s\le 11\frac{1}{17}$, откуда видим, что таких натуральных m нет, а из второго неравенства следует, что $s=11$. Значит, в первом столбике нет чисел, делящихся на 13, и имеется всего одно число $y=-119+510\cdot 11=5491$, делящееся на 17.

Замечание 2. Как было сказано ранее, все числа таблицы 4 можно было бы распределить по-другому, взяв, например, модуль $m=60$. Тогда мы получили бы таблицу 5.

Таблица 5

$K_1^{(60)}$	$K_7^{(60)}$	$K_{11}^{(60)}$	$K_{13}^{(60)}$	$K_{17}^{(60)}$	$K_{19}^{(60)}$	$K_{23}^{(60)}$	$K_{29}^{(60)}$	$K_{31}^{(60)}$	$K_{37}^{(60)}$	$K_{41}^{(60)}$	$K_{43}^{(60)}$	$K_{47}^{(60)}$	$K_{49}^{(60)}$	$K_{53}^{(60)}$	$K_{59}^{(60)}$
										5201	5203	5207	5209	5213	5219
5221	5227	5231	5233	5237	5239	5243	5249	5251	5257	5261	5263	5267	5269	5273	5279
5281	5287	5291	5293	5297	5299	5303	5309	5311	5317	5321	5323	5327	5329	5333	5339
5341	5347	5351	5353	5357	5359	5363	5369	5371	5377	5381	5383	5387	5389	5393	5399
5401	5407	5411	5413	5417	5419	5423	5429	5431	5437	5441	5443	5447	5449	5453	5459
5461	5467	5471	5473	5477	5479	5483	5489	5491	5497	5501	5503	5507	5509	5513	5519
5521	5527	5531	5533												

Эта таблица ничем не хуже предыдущей, за исключением наличия большего количества пустых клеточек.

Замечание 3. Интересен вопрос об арифметических прогрессиях, состоящих лишь из простых чисел. Понятно, что их разность d – четное число. Приведем примеры: 5, 11,

17, 23, 29; $d = 6$. Это единственная прогрессия с данной разностью, состоящая из пяти членов, так как среди любых последовательных пяти членов арифметической прогрессии один (и только один) делится на 5 (в нашей задаче мы обосновывали аналогичное утверждение для вычеркивания составных чисел). Будучи простым, этот член должен равняться числу 5, и понятно, что это число является первым в такой прогрессии. Остальные прогрессии с разностью 6 содержат максимум 4 члена (простых). Например, 251, 257, 263, 269; еще 1741, 1747, 1753, 1759. В нашей таблице 4 тоже видим две прогрессии с разностью 6, одна из них содержит три члена – 5407, 5413, 5419, а другая – четырехчленная: 5431, 5437, 5443, 5449.

В таблице 4 существуют и другие арифметические прогрессии, состоящие из одних простых чисел. Количество их членов n от трех до пяти, разность $d = 30;60;90;120;150;180$. Мы выписали их в таблице 6.

Таблица 6

d	n	Члены прогрессии
30	3	5419, 5449, 5479
60	3	5273, 5333, 5393
60	3	5381, 5441, 5501
90	3	5297, 5387, 5477
90	3	5303, 5393, 5483
90	3	5347, 5437, 5527
120	3	5231, 5351, 5471
120	3	5279, 5399, 5519
150	3	5231, 5381, 5531
30	4	5441, 5471, 5501, 5531
90	4	5233, 5323, 5413, 5503
90	4	5261, 5351, 5441, 5531
30	5	5273, 5303, 5333, 5363, 5393

Среди известных подобных прогрессий наибольшую длину имеет прогрессия, состоящая из 12 членов. Она была найдена В.А. Голубевым, ее первый член равен 23143, разность 30030 [5, с. 35].

Пока неизвестно, существует ли арифметическая прогрессия любой длины, состоящая из одних простых членов.

Заключение

Рассмотренный нами способ выделения простых чисел на отрезках натурального ряда является частичным случаем задачи о нахождении простых чисел в арифметических прогрессиях, так как каждый столбик в составленной таблице является арифметической прогрессией – подмножеством класса вычетов по выбранному модулю. Мы рассматривали классы, взаимно простые с модулем, а в них – конечные арифметические прогрессии, все их члены взаимно просты с модулем. Еще в 1788 г. Лежандр высказал предположение о том, что в каждой бесконечной арифметической прогрессии, в которой первый член взаимно прост с модулем, содержится бесконечное количество простых чисел. Эту теорему доказал Дирихле в 1837 г.

Простые числа оставались объектом исследования и в дальнейшем. Были получены важные результаты в этой области. Приведем некоторые из них, касающиеся те-

мы нашей работы.

Метод «решета» Эратосфена впервые модифицировал Лежандр (1798 г.), использовав при этом функцию Мебиуса. Применив новое «решето», он показал, что $\pi(x)=o(x)$, где $\pi(x)$ – количество простых чисел, не превышающих числа x [2, с. 38]. Это был один из первых важных результатов в исследовании функции $\pi(x)$.

Современные модификации этого метода принадлежат норвежским математикам В. Бруну (1920 г.) и А. Сельбергу (1947 г.), советскому математику Ю. Линнику [4, с. 6, 7, 15, 44].

Еще в 1737 г. Л. Эйлер доказал, что ряд величин, обратных к простым числам, расходится, что еще раз свидетельствует о бесконечности множества простых чисел. Но известно, что ряд $\sum_{n=1}^{\infty}\frac{1}{n^2}$ является сходящимся. Поэтому имеем, что в определенном смысле простые числа расположены гуще в натуральном ряду, чем квадраты целых чисел.

Природу функции $\pi(x)$ изучали многие математики. П.Л. Чебышев установил (1850 г.) асимптотический закон распределения простых чисел в натуральном ряду: $\lim\limits_{x\to\infty}\pi(x):\frac{x}{\ln x}=1$, то есть $\pi(x)\sim\frac{x}{\ln x}$. А в 1896 г. почти одновременно Адамар и Валле Пуссен доказали, использовав дзета-функцию Римана, что $\pi(x)\sim\int_2^x\frac{dt}{\ln t}$, причем погрешность при вычислениях с помощью интегрального логарифма меньше, чем дает функция $\frac{x}{\ln x}$ [2, с. 54]. В настоящее время установлено также много критериев простоты числа [6, с. 31–40].

Разные «решета» Бруна (двойные, тройные и вообще многократные) служат для «просеивания» чисел в арифметических прогрессиях с начальным членом $a>0$ и разностью $m>0$, где $(a,m)=1$. Этим же методом можно оценить сверху количество «близнецов» – пар простых чисел $p-2$ и p, где $p\le x$. Существует 152892 пары «близнецов» меньших, чем $x=30000000$ [5, с. 17]. Известны также очень большие «близнецы», например 8004119 и 8004121, 10006427 и 10006429, 1000000009649 и 1000000009651. Пока не установлено, является ли множество «близнецов» бесконечным. Но В. Брун доказал (в 1919 г.), что даже если это и так, то ряд, состоящий из обратных к ним чисел, является сходящимся. Это свидетельствует о том, что «близнецы» в натуральном ряду встречаются очень редко.

С использованием «решета» Сельберга доказана красивая теорема о простых числах в арифметических прогрессиях: если $1\le m<x$, $0\le a<m$, $(a,m)=1$, $\pi(x,m,a)$ – количество простых чисел в арифметической прогрессии с первым членом a и разностью m, не превосходящих числа x, то $\pi(x,m,a)<c\cdot\frac{x}{\varphi(m)\cdot\ln\frac{x}{m}}$, где c – некоторая абсолютная постоянная. Также установлено, что $\lim\limits_{x\to\infty}\frac{\pi(x,m,a)}{\pi(x)}=\frac{1}{\varphi(m)}$. Обратим внимание на то, что этот предел не зависит от a. Из этого следует, что все классы вычетов, взаимно простые с модулем, содержат асимптотически равное количество простых чисел.

Ю. Линник доказал, что существует такая абсолютная постоянная C_{50}, что для любого натурального m в каждом классе вычетов по модулю m, взаимно простом с m, имеется простое число $p < m^{C_{50}}$ [1, с. 94].

Общий член каждого класса вычетов по модулю m выражается линейной функцией от одной переменной, это частичный случай многочлена с целыми коэффициентами от одной переменной. По теореме Дирихле видим, что среди множества значений линейной функции $f(x)=a+mx$, где $(a,m)=1$, существует бесконечно много простых чисел. Закономерен вопрос о существовании хоть одного многочлена $f(x)\in Z[x]$, который при всех натуральных значениях x принимает только простые значения. Оказалось, что такого многочлена не существует: среди значений каждого многочлена $f(x)\in Z[x]$ с положительным старшим коэффициентом имеется бесконечное множество составных [1, с. 24, с. 117], [2, с. 18–19], [4, с. 18]. Но доказано, что существует такое вещественное $A>1$, что целая часть $\left[A^{3^n}\right]$ всегда проста [2, с. 19]. Отметим еще один интересный результат, полученный ленинградским математиком Ю.В. Матиясевичем: существует многочлен $f(x_1,x_2,...,x_n)$ с целыми коэффициентами такой, что множество его положительных значений совпадает с множеством простых чисел, когда переменные принимают все целые значения. В первой работе автора это был многочлен 21-й степени от 21 переменной [2, с. 19–20].

Мы привели лишь немногие из различных многочисленных результатов, которыми обогатилась теория чисел в последние десятилетия. Они очень интересны, как и предмет теории чисел в целом. Поэтому эта наука увлекает не только специалистов-математиков, но и любителей математики [3], сумевших увидеть ее красоту. И все же, несмотря на значительные достижения, с простыми числами связано значительно больше вопросов, нежели уже доказанных фактов, разрешенных проблем.

СПИСОК ЛИТЕРАТУРЫ

1. Виноградов, И.М. Основы теории чисел / И.М. Виноградов. – М.: Наука, 1981. – 182 с.
2. Воронин, С.М. Простые числа / С.М. Воронин. – М. :Знание, 1978. – 64с.
3. Орешкин, П. Восьмеричный путь к простым числам / П. Орешкин // Техника – молодежи. – 1970. – №2.– С.41–42.
4. Прахар, К. Распределение простых чисел / К. Прахар. – М. : Мир, 1967. – 512 с.
5. Серпинский, В. Что мы знаем и чего не знаем о простых числах / В. Серпинский. – М.-Л. : Физматгиз, 1963. – 92 с.
6. Трост, Э. Простые числа / Э. Трост. – М. : Физматгиз. – 1959. – 136 с.

K.F. Filozof. **The Method of Finding of Prime Numbers**

A method of finding of prime numbers on segments of natural sequence is considered in the article. It is based on the idea of Eratosthenes sieve. Set of numbers of the considered segment is divided into subsets (arithmetic progressions), which are contained in the residue classes with respect to modulo m. Optimum alternative is validated for selection of arithmetical progressions on this segment with difference 2≤m≤200, which allows to test primality of minimal sufficient quantity of numbers of the selected segment. The efficiency of the proposed method is illustrated.

Рукапіс паступіў у рэдкалегію 23.05.2012