AZƏRBAYCAN MİLLİ ELMLƏR AKADEMİASININ XƏBƏRLƏRİ
Fizika- riyaziyyat və texnika elmləri seriyası, 2004, №3

TRANSACTIONS OF THE NATIONAL ACADEMY OF SCIENCES OF AZERBAIJAN
Series of physical- mathematical and technical sciences, 2004, №3

ИЗВЕСТИЯ НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК АЗЕРБАЙДЖАНА
Серия физико-математических и технических наук, 2004, №3

УДК: 511.2

САБЗИЕВ Н.М.

АЛГОРИТМ ДЛЯ СОСТАВЛЕНИЯ ТАБЛИЦ ПРОСТЫХ ЧИСЕЛ И ПРОСТЫХ БЛИЗНЕЦОВ

Введение. Для информационной безопасности Интернет сети применяются различные алгоритмы криптографической шифровки. Один из широко распространенных алгоритмов является RSA алгоритм, который основывается на выборе достаточно больших простых чисел. Исследования методов и алгоритмов определения простых чисел был предметом изучения математиков многих поколений. Еще греческим математикам был известен способ выделения простых чисел из натурального ряда, получивший название Эратосфена решето. Фибоначчи был первым математиком указавшим, что для нахождения делителей числа n достаточно испытать делимость этого числа на простые числа не больше $\sqrt{n}$. Первые таблицы для факторизации чисел появились еще в XVII веке [1]. Факторизация чисел в пределах первых 10 миллионов натуральных чисел была осуществлена и опубликована в первой половине XIX века. В 1951 году была опубликована таблица простых чисел (Я. Кулик, Л. Полетти, Р. Портер) до 11 миллиона [2]. А в 1959 году К. Бейкер и Ф. Грунбергер составили микрофильм, содержащий все простые числа до 104395301 [2; 3].

Пара простых чисел, разностью 2, называется простыми близнецами. Составление таблиц, простых близнецов, также имеют определенный научно-практический интерес. Известно [2], что до 30 миллиона имеется 152892 таких чисел.

В данной работе, дается алгоритм для проверки простоты заданного натурального числа. На основе этого алгоритма может быть составлена таблица простых чисел и таблица простых близнецов, содержащие в любом наперед заданном интервале натурального ряда. В конце статьи приводится таблица простых чисел, содержащиеся в интервале $[2\times10^9; 2\times10^9+6000]$ и таблица простых близнецов, содержащиеся в интервале $[2\times10^9+6000; 2\times10^9+46000]$.

Пусть N множество всех натуральных чисел. Обозначим, $N(5) = N \bigcap \{n \geq 5, n \in N\}$. Очевидно

$$N(5) = \{6m-1, 6m, 6m+1, 6m+2, 6m+3, 6m+4\}_{m=1}^{\infty}.$$

Представляя в виде $6m = 2\cdot 3\cdot m$, $6m+2 = 2\cdot(3m+1)$, $6m+4 = 2\cdot(3m+2)$, $6m+3 = 3\cdot(2m+1)$, легко видеть, что эти числа кроме самого себя и единицы имеют другие делители, поэтому при всех $m \in N$ являются составными числами. В работе [4] доказаны следующие утверждения.

Теорема 1. *Если число $n = 6m+1\,(m \in N)$ составное, то существует хотя бы одна пара $k, t \in N$, такая, что либо*

$$6m+1 = (6k+1)(6t+1), \quad (t \leq k),$$

либо

$$6m+1 = (6k-1)(6t-1), \quad (t \leq k).$$

Теорема 2. *Если число $n = 6m-1\,(m \in N)$ составное, то существует хотя бы одна пара $k, t \in N$, такая что $6m-1 = (6k+1)(6t-1)$.*

Сначала рассмотрим первое утверждение. Пусть $n = 6m + 1\,(m \in N)$ составное число. Тогда по крайней мере справедливо одно из равенств $6m + 1 = 36kt + 6k + 6t + 1$, и $6m + 1 = 36kt - 6k - 6t + 1$ или соответственно, $m = 6kt + k + t$, $m = 6kt - k - t$. Отсюда

$$t = \frac{m-k}{6k+1}, \qquad t = \frac{m+k}{6k-1},$$

где соответственно, $k = 1,\ldots,k_0$ и $k = 1,\ldots,\nu_0$. Числа k_0 и ν_0 легко вычисляются из условия $k = t$, т.е.

$$k_0 = \left[\frac{-1+\sqrt{1+6m}}{6}\right], \qquad \nu_0 = \left[\frac{1+\sqrt{1+6m}}{6}\right].$$

Через квадратные скобки обозначаем целую часть выражения. Таким образом доказана следующая

Теорема 3. *Число $n = 6m + 1\,(m \in N)$ простое, если конечные последовательности рациональных выражений*

$$\left\{\frac{m-k}{6k+1}\right\}_{k=1}^{k_0} \quad и \quad \left\{\frac{m+k}{6k-1}\right\}_{k=1}^{\nu_0} \tag{1}$$

не содержат ни одного целого положительного элемента.

Теперь рассмотрим второе утверждение.

Пусть $n = 6m - 1\,(m \in N)$ составное число. Целесообразно в дальнейшем рассмотреть два варианта: $6m - 1 = (6k + 1)(6t - 1), \quad t \le k$ и $6m - 1 = (6k - 1)(6t + 1), \quad t \le k$.

Тогда при $t \le k$ либо $6m - 1 = 36kt - 6k + 6t - 1$, либо $6m + 1 = 36kt + 6k - 6t - 1$ или соответственно, $m = 6kt - k + t$ или $m = 6kt + k - t$. Отсюда

$$t = \frac{m+k}{6k+1} \quad \text{или} \quad t = \frac{m-k}{6k-1},$$

где $k = 1,\ldots,r_0$. Число r_0 также вычисляется из условия $k = t$, т.е.

$$r_0 = \left[\frac{\sqrt{m}}{6}\right].$$

Таким образом доказана следующая

Теорема 4. *Число $n = 6m - 1\,(m \in N)$ простое, если конечные последовательности рациональных выражений*

$$\left\{\frac{m+k}{6k+1}\right\}_{k=1}^{r_0} \quad и \quad \left\{\frac{m-k}{6k-1}\right\}_{k=1}^{r_0} \tag{2}$$

не содержат ни одного целого положительного элемента.

Очевидно, что простые близнецы образуются из пары простых чисел $6m - 1$ и $6m + 1$ при тех значениях $m \in N$, когда эти числа одновременно простые. Следовательно справедлива

Теорема 5. *Числа $6m - 1$, $6m + 1$ $(m \in N)$ образуют пару простых близнецов, если одновременно выполняются условия теорем 1 и 2.*

Таким образом, процесс проверки простоты заданного натурального числа сведена проверке целостности и положительности элементов последовательностей (1) и (2). Приведем программу составления таблицы простых чисел, написанной на Паскале. Аналогичным образом составлена программа для составления таблицы простых блезнецов. Результат вычислений приводится в конце работы (Таблицы 1, 2).

```
procedure Sade_aded;
```

```
Var     M0,M1, m, r0, n0, k0, j          : Longint;
        e, e1,e2                         : Double;
Begin
      Readln (M0);
      Readln (M1);
      M0:=trunc((M0+1)/6);
      M1:=trunc((M1+1)/6);
      For m:=M0 to M1 do
      Begin
            r0:=trunc(sqrt(m/6));
            j:=1;
            e1:=1;
            e2:=1;
            While (j<=r0)and(e1*e2<>0) do
            Begin
                  e1:=Frac((m+j)/(6*j+1));
                  e2:=Frac((m-j)/(6*j-1));
                  j:=j+1;
            end;
            if (e1*e2<>0) then Writeln(6*m-1);
            n0:=trunc((sqrt(6*m+1)+1)/6);
            k0:=trunc((sqrt(6*m+1)-1)/6);
            j:=1;
            e:=1;
            while (j<=n0)and(e<>0) do
            Begin
                  e:=Frac((m+j)/(6*j-1));
                  j:=j+1;
            end;
            if (e<>0) then
            Begin
                  j:=1;
                  e:=1;
                  while (j<=k0)and(e<>0) do
                  Begin
                        e:=Frac((m-j)/(6*j+1));
                        j:=j+1;
                  end;
                  if (e<>0) then Writeln(6*m+1);
            end;
      end;
end.
```

Таблица 1. Простые числа, содержащиеся в интервале $[2\times10^9; 2\times10^9+6000]$.

2000000011	2000000843	2000001953	2000003053	2000004043	2000005087
2000000033	2000000957	2000001973	2000003077	2000004079	2000005093
2000000063	2000000983	2000002031	2000003081	2000004109	2000005099
2000000087	2000001001	2000002061	2000003107	2000004143	2000005211
2000000089	2000001013	2000002091	2000003123	2000004161	2000005219
2000000099	2000001043	2000002129	2000003141	2000004199	2000005223
2000000137	2000001049	2000002133	2000003149	2000004217	2000005229
2000000141	2000001089	2000002153	2000003153	2000004233	2000005237
2000000143	2000001097	2000002171	2000003209	2000004241	2000005247
2000000153	2000001103	2000002177	2000003219	2000004257	2000005261
2000000203	2000001109	2000002183	2000003227	2000004263	2000005277
2000000227	2000001119	2000002217	2000003231	2000004269	2000005279
2000000239	2000001127	2000002259	2000003261	2000004319	2000005313
2000000243	2000001137	2000002261	2000003273	2000004329	2000005321
2000000269	2000001149	2000002267	2000003281	2000004359	2000005327
2000000273	2000001151	2000002271	2000003293	2000004367	2000005351
2000000279	2000001167	2000002273	2000003303	2000004371	2000005367
2000000293	2000001173	2000002289	2000003333	2000004403	2000005369
2000000323	2000001187	2000002297	2000003351	2000004421	2000005421
2000000333	2000001229	2000002307	2000003353	2000004431	2000005451
2000000357	2000001233	2000002321	2000003359	2000004443	2000005453
2000000381	2000001247	2000002331	2000003407	2000004473	2000005459
2000000393	2000001257	2000002343	2000003413	2000004481	2000005499
2000000407	2000001277	2000002379	2000003431	2000004493	2000005507
2000000413	2000001287	2000002439	2000003449	2000004521	2000005529
2000000441	2000001349	2000002441	2000003459	2000004551	2000005589
2000000503	2000001359	2000002457	2000003491	2000004553	2000005591
2000000507	2000001379	2000002469	2000003501	2000004557	2000005639
2000000531	2000001413	2000002507	2000003503	2000004563	2000005663
2000000533	2000001457	2000002531	2000003519	2000004571	2000005669
2000000579	2000001511	2000002597	2000003527	2000004607	2000005673
2000000603	2000001517	2000002619	2000003543	2000004659	2000005697
2000000609	2000001527	2000002679	2000003569	2000004679	2000005717
2000000621	2000001539	2000002717	2000003591	2000004701	2000005729
2000000641	2000001551	2000002721	2000003623	2000004709	2000005751
2000000659	2000001557	2000002787	2000003627	2000004719	2000005823
2000000671	2000001583	2000002801	2000003651	2000004781	2000005829
2000000693	2000001599	2000002813	2000003699	2000004821	2000005831
2000000707	2000001623	2000002819	2000003701	2000004829	2000005837
2000000731	2000001629	2000002831	2000003729	2000004857	2000005877
2000000741	2000001649	2000002841	2000003741	2000004889	2000005879
2000000767	2000001677	2000002843	2000003779	2000004913	2000005883
2000000771	2000001727	2000002853	2000003807	2000004953	2000005907
2000000773	2000001743	2000002931	2000003861	2000004973	2000005913
2000000789	2000001821	2000002969	2000003867	2000004983	2000005957
2000000797	2000001833	2000002987	2000003891	2000004991	2000005961
2000000809	2000001851	2000002993	2000003963	2000005003	2000005999
2000000833	2000001881	2000003039	2000003983	2000005013	
2000000837	2000001929	2000003051	2000004023	2000005019	

Таблица 2. Простые близнецы, содержащиеся в интервале $[2\times10^9+6000; 2\times10^9+46000]$.

2000006681	2000012471	2000017937	2000026979	2000033939	2000040851

2000006683	2000012473	2000017939	2000026981	2000033941	2000040853
2000006717	2000012951	2000018309	2000027387	2000034401	2000041037
2000006719	2000012953	2000018311	2000027389	2000034403	2000041039
2000006891	2000013089	2000018861	2000028389	2000034539	2000041247
2000006893	2000013091	2000018863	2000028391	2000034541	2000041249
2000007221	2000013149	2000018927	2000028467	2000034767	2000041271
2000007223	2000013151	2000018929	2000028469	2000034769	2000041273
2000007641	2000013341	2000019011	2000029061	2000035001	2000041361
2000007643	2000013343	2000019013	2000029063	2000035003	2000041363
2000007767	2000013437	2000019521	2000029079	2000035379	2000041469
2000007769	2000013439	2000019523	2000029081	2000035381	2000041471
2000007851	2000013557	2000019557	2000029217	2000036429	2000042327
2000007853	2000013559	2000019559	2000029219	2000036431	2000042329
2000008097	2000014061	2000019977	2000029817	2000037041	2000042519
2000008099	2000014063	2000019979	2000029819	2000037043	2000042521
2000008499	2000014097	2000020151	2000029859	2000037239	2000042729
2000008501	2000014099	2000020153	2000029861	2000037241	2000042731
2000008601	2000014559	2000021249	2000030189	2000037311	2000043041
2000008603	2000014561	2000021251	2000030191	2000037313	2000043043
2000008709	2000014661	2000021267	2000030651	2000037497	2000043587
2000008711	2000014663	2000021269	2000030653	2000037499	2000043589
2000008937	2000014739	2000021381	2000030777	2000037581	2000043809
2000008939	2000014741	2000021383	2000030779	2000037583	2000043811
2000009057	2000015291	2000021981	2000031377	2000037797	2000043971
2000009059	2000015293	2000021983	2000031379	2000037799	2000043973
2000009129	2000015681	2000022929	2000031497	2000038739	2000044619
2000009131	2000015683	2000022931	2000031499	2000038741	2000044621
2000009327	2000016671	2000024051	2000031959	2000038877	2000044691
2000009329	2000016673	2000024053	2000031961	2000038879	2000044693
2000009927	2000017181	2000024249	2000032421	2000038979	2000045237
2000009929	2000017183	2000024251	2000032423	2000038981	2000045239
2000010821	2000017301	2000024597	2000032481	2000039231	2000045387
2000010823	2000017303	2000024599	2000032483	2000039233	2000045389
2000011217	2000017337	2000024669	2000032631	2000040059	2000045501
2000011219	2000017339	2000024671	2000032633	2000040061	2000045503
2000011931	2000017541	2000025497	2000032787	2000040101	
2000011933	2000017543	2000025499	2000032789	2000040103	
2000012321	2000017757	2000026739	2000033489	2000040269	
2000012323	2000017759	2000026741	2000033491	2000040271	

ЛИТЕРАТУРА

1. *Бухштаб А.А.* Теория чисел. М., Наука, 1966.
2. *Виноградов П.М.* Метод тригонометрических сумм в теории чисел. М., Наука, 1980.
3. Диамонд Г. Элементарные методы в изучении распределения простых чисел. УМН. т.46, вып. 2 (272), 1990.
4. *Сабзиев Н.М.* Свойство множеств порождающие составные числа вида $6m \pm 1$. Известия НАН Азербайджана, Серия физ.-тех.и матем.наук, Т.XXIII № 3, 2003, С.41-49.

Баку, Комп.Кибер Ltd

Представлено 270504