Потоскуев Сергей Эрвинович
канд. физ.-мат. наук, доцент
Нижнетагильский филиал
ГАОУ ДПО СО «Институт развития образования»
г. Нижний Тагил, Свердловская область

О СОДЕРЖАНИИ ПРОЕКТНОЙ ДЕЯТЕЛЬНОСТИ УЧАЩИХСЯ ПО МАТЕМАТИКЕ

Аннотация: *в статье говорится об одной из наиболее важных проблем организации проектной учебно-исследовательской деятельности в школе является выбор направления и тематики проектов учащихся. Поставленная задача должна быть посильна для юного исследователя, но при этом по своему содержанию требовать от ученика активных усилий по освоению материала выбранной предметной области, инициативного поиска неординарных решений, опираясь на всю совокупность имеющихся у него знаний.*

Ключевые слова: *численный метод, простое число, ключ, произведение чисел, факторизация, разложение на простые множители, алгоритм шифрования, итерация.*

Как показывает опыт, хороший школьный исследовательский проект почти всегда, по своему содержанию, выходит за границы учебника, и зачастую включает сведения из смежных предметных областей. Проектная деятельность в области математики обладает в этом отношении своей спецификой: учащимся сложно реализовать самостоятельный исследовательский компонент, в силу чего вся деятельность сводится к более широкому (или глубокому) освоению той или иной темы. В случае, если данная работа проделана учащимися честно и осознанно, такие проекты являются, несомненно, полезными. Однако практика свидетельствует, что настоящий образовательный результат может быть получен только в случае положительной мотивационной составляющей в самом характере деятельности, что довольно трудно реализовать в рамках обычного выучивания дополнительного материала и составления доклада. Включение учащегося

в непосредственно продуктивную деятельность при исполнении проекта по математике является естественной основной формирования такой положительной мотивации. Покажем на примере, как это можно реализовать.

Разложение произведения на простые множители

Очень важно ясно сформулировать актуальность задачи разложения на простые множители, объяснив учащимся насколько широко сегодня применяются методы асимметричного шифрования и показав прямую связь свойств простых чисел и реализации основных алгоритмов защиты конфиденциальности на примере генерации ключей по схеме Ривеста-Шамира-Адлемана [РША]. Данная схема чрезвычайно проста и доступна школьнику, но при своей реализации производит совершенно магическое впечатление.

Необходимо объяснить учащимся, что задача факторизации (разложения на простые множители) является одной из фундаментальных проблем математики и к настоящему времени разработаны алгоритмы, позволяющие с достаточной эффективностью добиваться результата за приемлемое время (алгоритмы). Все они основаны на так называемых численных методах решения математических задач, а для их понимания необходима очень серьезная математическая подготовка, а некоего общего алгоритма, работающего одинаково быстро для задач разного класса сложности, просто не существует. На данном этапе учащиеся должны разобраться с принципами численного решения задач, которые весьма просты для понимания. Важно, чтобы юные исследователи осознали тот факт, что в большинстве случаев формализованного описания реальных процессов и проведения точных расчетов применяются именно численные методы, поскольку строго аналитически сделать это не удается.

Несмотря на указанную сложность проблемы факторизации, можно попытаться найти способ сокращения времени перебора множителей, учитывая тот факт, что для прикладных задач шифрования чаще всего используются произведения двух чисел, одинаковых по порядку величины. На данном этапе обсуждения учитель должен с помощью наводящих вопросов, небольших подсказок и

одобрения верных догадок учащихся, подвести их к геометрическому смыслу произведения двух чисел – площади прямоугольника.

$$S = a \times b \quad (1)$$

Это, во-первых, позволит учащимся осознать единство математики (что не менее важно, чем конкретный прикладной результат), и во-вторых сразу приводит к мысли о необходимости каким-то образом найти периметр для получения системы уравнений, разрешимой относительно неизвестных сомножителей:

$$\begin{cases} S = a \times b \\ P = 2 \times (a + b) \end{cases} \quad (2)$$

Очевидно, что прямоугольники, имеющие одинаковый периметр, но разное соотношение сторон (k), имеют площади, пропорциональные этому отношению:

$$S = k \times a^2 \ (b = k \times a) \quad (3)$$

Максимальное значение площади (A) будет у квадрата со стороной

$$l = \frac{a+b}{2} \quad (4)$$

$$A = \frac{(a+b)^2}{4} \quad (5)$$

Чем меньше отличаются стороны прямоугольника, тем ближе значение его площади к максимальному, т. е. площади квадрата с тем же периметром. С точки зрения числового ряда это означает, что соответствующие числа расположены недалеко друг от друга.

Алгоритм поиска площади квадрата с тем же периметром, что и прямоугольник, площадь которого нам известна, может быть следующим.

Из соотношения (5) следует, что

$$a \times b = 2 \times \sqrt{A} \quad (6)$$

Учитывая, что

$a \times b = S$, т. е.

$$b = \frac{S}{a}$$

Получаем простое квадратное уравнение:

$$a^2\text{-}2 \times a \times \sqrt{A} + S = 0 \quad (7)$$

В случае, если значения площадей S и A найдены правильно, его корнями будут искомые числа a и b:

$$a, b = \sqrt{A} \pm \sqrt{A\text{-}S} \quad (8).$$

Осталось найти значение A методом численного подбора. Поскольку, как отмечалось выше, величины A и S отличаются незначительно, начать эту операцию нужно с числа, равного целой части $\sqrt{S}$. Затем, добавляя 1, получаем промежуточное значение A и вычисляем дискриминант $\sqrt{A\text{-}S}$. Пока полученное значение не окажется целым, операция добавления единицы повторяется.

Таким образом, алгоритм построения программы выглядит следующим образом:

1) вычисление значения $A_{\text{промежуточное}} = \sqrt{S}$,

2) округление данного значения до целого,

3) увеличение полученного значения на 1,

4) вычисление дискриминанта $\sqrt{A_{\text{промежуточное}}\text{-}S}$,

5) проверка на целое полученного числа,

6) если дискриминант не является целым (а так поначалу и будет), округляем его до целого и снова увеличиваем значение на 1.

Реализация данного алгоритма может быть осуществлена различными программными средствами, а простота позволяет использовать даже стандартные приложения, такие как электронные таблицы. Рассмотрим это можно сделать в Microsoft Excel.

В соответствии с изложенными выше шагами, необходимо, прежде всего, задать столбцы для последовательной записи результатов вычислений, и взять два достаточно больших простых числа, расположенных как можно ближе достаточно близко на числовой оси. Сетевые ресурсы позволяют легко подобрать, например, шестизначные числа a и b: … 999671, 999683, 999721, 999727, 999749, 999763, 999769, 999773, 999809, 999853, 999863, 999883, 999907, 999917, 999931, 999953, 999959, 999961, 999979, 999983…

Ниже представлен фрагмент таблицы Excel с заполненными столбцами. В качестве исходных чисел выбраны 999961 и 999983. Видно, что разложение на множители происходит уже на первом шаге итерации, что неудивительно, поскольку исходные числа располагаются на числовой оси так, что разделены всего одним числом – 999979, а их разность составляет 22 единицы. Очевидно, что в случае прямого перебора программа должна была бы совершить несколько сотен тысяч итераций.

B2 =B3*B4

	A	B	C	D	E	F	G	H	I	J	K	L	M
1		Число (S)	Корень из числа (S)	Округление и увеличение на 1	Перебор A	Дискриминант (A-S)	Корень (A-S)	Перебор a	Перебор b	Остаток a	Остаток b	a	b
2		999944000663,0	999971,9999	999972	999944000784,0	121,0	11,0000	999983,0000	999961,0000	0	0	999983	999961
3	a	999983		999973	999946000729,0	2000066,0	1414,2369	1001387,237	998558,7631	0,236896704	0,7631033	-	-
4	b	999961		999974	999948000676,0	4000013,0	2000,0032	1001974,003	997973,9968	0,003249997	0,99675	-	-

Интересно исследовать, как поведет себя алгоритм, если числа, выступающие в качестве сомножителей, будут отличаться на большее число единиц, например, 4662 = 999671 – 995009.

D9 =D8+1

	A	B	C	D	E	F	G	H	I	J	K	L	M
1		Число (S)	Корень из числа (S)	Округление и увеличение на 1	Перебор A	Дискриминант (A-S)	Корень (A-S)	Перебор a	Перебор b	Остаток a	Остаток b	a	b
2		994681642039,0	997337,2760	997338	994683086244,0	1444205,0	1201,7508	998539,7508	996136,2492	0,750806116	0,2491939	-	-
3	a	999671		997339	994685080921,0	3438882,0	1854,4223	999193,4223	995484,5777	0,422282006	0,577718	-	-
4	b	995009		997340	994687075600,0	5433561,0	2331,0000	999671	995009	0	0	999671	995009

Как видим, потребовалось всего три шага. Вообще, задача установления зависимости количества итераций, необходимых для получения результата, от номера исходных чисел в числовом ряду (ограничиваясь его нечетной составляющей), представляет самостоятельный интерес и может стать одним из направлений дальнейшего исследования свойств данного алгоритма. Если, например, разность составляет уже 15024 единицы, т.е. исходные числа 999983 и 984959, наш алгоритм находит решение на 30 шаге:

	A	B	C	D	E	F	G	H	I	J	K	L	M
1		Число (S)	Корень из числа (S)	Округление и увеличение на 1	Перебор A	Дискриминант (A-S)	Корень (A-S)	Перебор a	Перебор b	Остаток a	Остаток b	a	b
2		984942255697,0	992442,5705	992443	984943108249,0	852552,0	923,3374	993366,3374	991519,6626	0,33742478	0,6625752	-	-
3	a	999983		992444	984945093136,0	2837439,0	1684,4699	994128,4699	990759,5301	0,469946304	0,5300537	-	-
4	b	984959		992445	984947078025,0	4822328,0	2195,9800	994640,98	990249,02	0,979963479	0,0200365	-	-
5		15024		992446	984949062916,0	6807219,0	2609,0648	995055,0648	989836,9352	0,064774972	0,935225	-	-
6				992447	984951047809,0	8792112,0	2965,1496	995412,1496	989481,8504	0,149574642	0,8504254	-	-
7				992448	984953032704,0	10777007,0	3282,8352	995730,8352	989165,1648	0,835207561	0,1647924	-	-
8				992449	984955017601,0	12761904,0	3572,3807	996021,3807	988876,6193	0,380718792	0,6192812	-	-
9				992450	984957002500,0	14746803,0	3840,1566	996290,1566	988609,8434	0,15663743	0,8433626	-	-
10				992451	984958987401,0	16731704,0	4090,4406	996541,4406	988360,5594	0,440563069	0,5594369	-	-
11				992452	984960972304,0	18716607,0	4326,2694	996778,2694	988125,7306	0,269409087	0,7305909	-	-
12				992453	984962957209,0	20701512,0	4549,8914	997002,8914	987903,1086	0,891427276	0,1085727	-	-
13				992454	984964942116,0	22686419,0	4763,0262	997217,0262	987690,9738	0,026243892	0,9737561	-	-
14				992455	984966927025,0	24671328,0	4967,0241	997422,0241	987487,9759	0,02405873	0,9759413	-	-
15				992456	984968911936,0	26656239,0	5162,9680	997618,968	987293,032	0,968041737	0,0319583	-	-
16				992457	984970896849,0	28641152,0	5351,7429	997808,7429	987105,2571	0,742893675	0,2571063	-	-
17				992458	984972881764,0	30626067,0	5534,0823	997992,0823	986923,9177	0,082308748	0,9176913	-	-
18				992459	984974866681,0	32610984,0	5710,6028	998169,6028	986748,3972	0,602770286	0,3972297	-	-
19				992460	984976851600,0	34595903,0	5881,8282	998341,8282	986578,1718	0,828202183	0,1717978	-	-
20				992461	984978836521,0	36580824,0	6048,2083	998509,2083	986412,7917	0,208329745	0,7916703	-	-
21				992462	984980821444,0	38565747,0	6210,1326	998672,1326	986251,8674	0,13260728	0,8673927	-	-
22				992463	984982806369,0	40550672,0	6367,9410	998830,941	986095,059	0,9409545	0,0590455	-	-
23				992464	984984791296,0	42535599,0	6521,9322	998985,9322	985942,0678	0,932152361	0,0678476	-	-
24				992465	984986776225,0	44520528,0	6672,3705	999137,3705	985792,6295	0,370493311	0,6295067	-	-
25				992466	984988761156,0	46505459,0	6819,4911	999285,4911	985646,5089	0,491110046	0,50889	-	-
26				992467	984990746089,0	48490392,0	6963,5043	999430,5043	985503,4957	0,504290226	0,4957098	-	-
27				992468	984992731024,0	50475327,0	7104,5990	999572,599	985363,401	0,599003462	0,4009965	-	-
28				992469	984994715961,0	52460264,0	7242,9458	999711,9458	985226,0542	0,945809545	0,0541905	-	-
29				992470	984996700900,0	54445203,0	7378,6993	999848,6993	985091,3007	0,699275618	0,3007244	-	-
30				992471	984998685841,0	56430144,0	7512,0000	999983	984959	0	0	999983	984959

Предлагаемый нами подход к изучению математики через деятельность на основе имеющихся знаний по информатике, позволяет существенно расширить область понимания учащимися возможностей численных методов и сформировать их мотивацию к дальнейшей исследовательской работе в этом направлении.

Обсуждаемая задача взята нами в качестве наглядного примера того, как достаточно простыми средствами можно представить весьма фундаментальные математические проблемы на уровне школьного знания в рамках организации проектной деятельности учащихся.