точности числа, взаимно простые с 12, и что незачеркнутые числа не образуют решетки.

б) Докажите теорему Эйлера по следующему плану:

1) числа, взаимно простые с n, заполняют собой $\varphi(n)$ столбцов таблицы 9;

2) остатки от деления на m всех m чисел любого столбца таблицы 9 различны;

3) в каждом столбце присутствует ровно $\varphi(m)$ чисел, взаимно простых с m;

4) число взаимно просто с mn тогда и только тогда, когда оно взаимно просто с n (такие числа лежат в $\varphi(n)$ столбцах) и взаимно просто с m (в каждом столбце таких чисел $\varphi(m)$).

40. Окружность разделили n точками на n равных частей. Сколько можно построить различных замкнутых ломаных из n равных звеньев с вершинами в этих точках? (Две ломаные, получающиеся одна из другой поворотом, считаем одинаковыми. На рисунке 1 изображены все такие ломаные при $n = 20$.)

41. Для любых натуральных чисел m и n докажите равенства:

а) $\varphi(m)\varphi(n) = \varphi(\text{НОК}(m,n))\varphi(\text{НОД}(m,n))$;

б) $\varphi(mn) = \varphi(\text{НОК}(m,n)) \cdot \text{НОД}(m,n)$;

в) $\varphi(m)\varphi(n)\text{НОД}(m,n) = \varphi(mn)\varphi(\text{НОД}(m,n))$.

г) Пусть m и n – натуральные числа, причем $\text{НОД}(m,n) > 1$. Докажите неравенство $\varphi(mn) > \varphi(m)\varphi(n)$.

42. Решите уравнения: а) $\varphi(x) = 18$; б) $\varphi(x) = 12$; в) $x - \varphi(x) = 12$; г*) $\varphi(x^2) = x^2 - x$; д) $\varphi(x) = x/2$; е) $\varphi(x) = x/3$; ж*) $\varphi(x) = x/n$, где n – натуральное число, $n > 3$; з) $\varphi(nx) = \varphi(x)$, где n – натуральное число, $n > 1$.

Шифры с открытым ключом

На вопрос, что он написал в шифровке, Штирлиц ответил: «Не помню. Теперь это знает только Центр.»

Вообразите, что вам нужно получить зашифрованное сообщение от вашего друга, но вы с ним не договорились заранее, каким шифром будете пользоваться. Как быть? Существует ли такой метод шифрования, что его можно сообщить всему миру (в том числе и вашему другу, и врагам), но это не даст врагам возможности расшифровать сообщение?

Это был бы замечательный шифр: в отличие от старых шифров, где главный секрет – ключ, знание которого позволяет и зашифровывать, и расшифровывать сообщения, новый шифр – «с открытым ключом»: каждый может зашифровывать, но только автор шифра может расшифровать получаемые сообщения.

Шифр RSA

...Так начались необычайные события, которые вовлекли в свой круговорот немало людей.

Е.Велтистов

Скорее всего, шифр с открытым ключом уже изобретен! В 1978 году три математика – Ривест, Шамир и Адлеман – зашифровали некоторую английскую фразу и пообещали награду в 100$ первому, кто расшифрует сообщение

$$y = 96869613754622061477140922254355882905759991124574319874695120930816298225145708356931476622883989628013391990551829945157815154.$$

Они подробно объяснили способ шифрования. Сначала фразу бесхитростно (a = 01, b = 02, c = 03,..., z = 26, пробел = 00) записали в виде последовательности цифр. Получилось некоторое 78-значное число x. Затем взяли 64-значное простое число p и 65-значное простое число q. Перемножили их (не вручную, разумеется, а на компьютере):

$$pq = 114381625757888867669325779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541.$$

Теперь – главное:

$$y \equiv x^{9007} \pmod{pq}.$$

Понимаете? Они опубликовали и произведение pq, и число 9007, и сам метод шифрования (и, разумеется, число y). Было даже сказано, что из чисел p и q одно 64-значное, а другое 65-значное. В секрете остались только сами числа p и q. Требовалось найти x.

Эта история завершилась в 1994 году, когда Аткинс, Крафт, Ленстра и Лейланд расшифровали эту фразу. Числа p и q оказались равны

$$p = 3490529510847650949147849619903898133417764638493387843990820577,$$

$$q = 32769132993266709549961988190834461413177642967992942539798288533.$$

В книге «Введение в криптографию» (М., МЦНМО, 1998 г.) сказано: «Этот замечательный результат (разложение на множители 129-значного числа) был достигнут благодаря использованию алгоритма разложения чисел на множители, называемого методом квадратичного решета. Выполнение вычислений потребовало колоссальных ресурсов. В работе, возглавлявшейся четырьмя авторами проекта и продолжавшейся после предварительной теоретической подготовки примерно 220 дней, на добровольных началах участвовало около 600 человек и примерно 1600 компьютеров, объединенных сетью Internet.»

К сожалению, рассказ о методе квадратичного решета увел бы нас далеко в сторону от основной темы. Потому оставим его до лучших времен, а здесь обсудим основную идею системы RSA (по первым буквам фамилий авторов: Rivest, Shamir, Adleman).

Идея очень красива. Во-первых, зная p и q, можно найти $\varphi(pq) = (p-1)(q-1)$. Во-вторых (и это главное!), если

$$ef = 1 + k\varphi(pq),$$

где e, f, k – натуральные числа, то для любого числа x, взаимно простого с pq, по теореме Эйлера имеем

$$x^{ef} = x \cdot \left(x^k\right)^{\varphi(pq)} \equiv x \cdot 1 = x \pmod{pq}.$$

Вы поняли, что такое e и f? В нашем примере $e = 9007$ (единственное обязательное математическое требование к числу e – его взаимная простота с числом $(p-1)(q-1)$; впрочем, брать $e = 1$ или $e = (p-1)(q-1) - 1$ вряд ли разумно, если хотите сохранить секреты). А число f, как уже было сказано, – решение сравнения

$$ef \equiv 1 \pmod{\varphi(pq)}.$$

(В *Приложении* рассказано, как алгоритм Евклида позволяет решать такие сравнения.)