штук в кубическом метре, но все они одинаковы и находятся в среднем на одном и том же расстоянии друг от друга — порядка $1/\sqrt[3]{N}$. И в результате найдем некоторую эффективную, или среднеобъемную, диэлектрическую проницаемость такой пузырьковой жидкости. Но даже эту скромную программу выполнить не очень легко, да это и не обязательно делать сейчас до конца – на основе двух рассмотренных выше примеров ясно, что результат будет зависеть от суммарного объема пузырьков, попавших в конденсатор, и что временна́я зависимость тока будет скорее всего иной, чем в упомянутых примерах.

А что еще мы не учли в этих случаях? Многое. Например, что диэлектрик втягивается в конденсатор. Это значит, что в первом случае «снарядного» течения газовый пузырь, попавший в конденсатор, будет сжиматься слева и справа двумя пробками жидкости. То же самое будет происходить и с пузырьковой жидкостью, если суммарный объем пузырьков будет непостоянен в пространстве, так что движение такой газожидкостной смеси в конденсаторе не будет равномерным.

Далее, в реальности существует сопротивление проводов и внутреннее сопротивление источника напряжения. Если их сумма равна r, то разность потенциалов между пластинами конденсатора запишется в виде

$$\frac{q}{C(t)} = U - rI(t)$$

и уже не будет постоянной величиной. А если учесть еще индуктивность цепи L и соответствующую ей ЭДС самоиндукции $-L\dfrac{dI}{dt}$, то закон Кирхгофа даст страшное дифференциальное уравнение для заряда:

$$L\frac{d^2q}{dt^2} + r\frac{dq}{dt} + \frac{q}{C(t)} = U,$$

которое описывает затухающие колебания. Решить это уравнение сложно, так как емкость конденсатора изменяется со временем (в этом-то и состоит суть метода), но можно ожидать, что на вышенарисованные кривые зависимости заряда и тока от времени налажатся «гармошки» колебаний (см. рис.2, точечные кривые).

Кроме того, можно предложить и другую схему измерений. Например, зарядить конденсатор от какого-либо источника, затем отключить последний и сохранять на пластинах постоянный заряд (вот тут-то и пригодится пренебрежимо малая электропроводность жидкости). Тогда при прохождении через конденсатор жидкости с различным содержанием газа в пузырьках будет изменяться разность потенциалов между пластинами. Такие приборы существуют и называются *емкостными датчиками.*

Надо признаться, что такими способами мы найдем только суммарный относительный объем газовой фазы, а не концентрацию пузырьков. Не худо было бы определить как-нибудь и их средний размер. Нужно, следовательно, использовать еще какие-то физические явления и приборы (например, оптические)... Так что, прежде чем открыть бутылку нарзана, подумайте о числе пузырьков и законах физики. И – приятного аппетита!

Малая теорема Ферма

(Начало см. на с. 9)

последнего уравнения. Зная x и y, легко находим

$$d = x + y = 9,\quad c = x + 6d = 62,\quad b = d + 5c = 319,$$

$$a = b + c = 381,\quad k = b + 4a = 1843,\quad f = a + 2k = 4067.$$

Победа! Числа k и f найдены! (Проверка: $9007 \cdot 4067 = 36631469 = 1 + 19876 \cdot 1843$.)

Упражнение 44* (для тех, кто очень любит программировать). а) Найдите число f, которое нашли Аткинс, Крафт, Ленстра и Лейланд. б) Расшифруйте фразу, зашифрованную в 1978 году Ривестом, Шамиром и Адлеманом.

Что дальше?

Что остается от сказки потом,
После того, как ее рассказали?
В.Высоцкий

Подытожим. В первой части статьи мы доказали малую теорему Ферма и ее обобщение – теорему Эйлера. Рассказали о практическом применении теоремы Эйлера в криптографии. Правда, осталось тайной, откуда взялись числа p, q (точнее говоря, как можно конструировать большие – в несколько десятков или сотен цифр – простые числа).

Во второй части мы расскажем об основанных на малой теореме Ферма методах конструирования больших простых чисел. Расскажем и о числах Кармайкла, история которых началась в древности, а существование бесконечного множества которых доказано в 1994 году.

Малую теорему Ферма не обязательно доказывать именно так, как это сделано выше. Во второй части мы изложим другие способы. Один из них приведет к теореме о существовании первообразного корня по простому модулю и далее – к теореме о строении мультипликативной группы вычетов по (не обязательно простому) модулю n.

Чтобы вы лучше оценили силу результатов второй части статьи, подумайте над следующими задачами. Все они будут решены во второй части. Не огорчайтесь даже в том случае, если ни одна из них не получится: это не упражнения, а довольно трудные задачи!

Задачи

1. Существует ли такое составное число n (число Кармайкла), что для любого целого числа a разность $a^n - a$ кратна n?

2. Ни для какого натурального числа n число $2^n + 1$ не кратно $n + 1$. Докажите это.

3. Если $2^n + 1$ кратно n, то $n = 1$ или n кратно 3. Докажите это.

4. Для каких n числа $1, 2, \ldots, n-1$ можно расставить вдоль окружности так, чтобы для любых подряд идущих чисел a, b, c разность $b^2 - ac$ была кратна n? (На рисунке 2 изображен случай $n = 7$.)

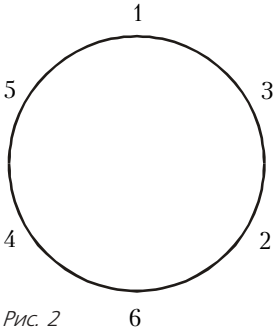

Рис. 2

5. Для каких простых чисел p существует такое целое число a, что $a^4 + a^3 + a^2 + a + 1$ кратно p?