18 Генерация простых

Задача. Боб генерирует простые числа, используя теорему Диемитко: если q — нечетное простое, R – четное, $R < 4(q+1)$, $n = qR + 1$ и для некоторого целого a выполняются условия:

1) n делит $a^{qR} - 1$;

2) n не делит $a^R - 1$,

то n — простое.

Для построения простого n битовой длины k ($2^{k-1} < n < 2^k$) Боб находит $[k/2]$-битовое простое q (выбирает малое простое или генерирует q снова с помощью теоремы Диемитко). Затем Боб выбирает четное R так, что $n = qR + 1$ имеет нужную длину k и проверяет условия 1) и 2) для случайного a.

Алгоритм Боба содержит ошибку. Найдите составное n, которое Боб может признать простым.

Решение. Докажем сначала теорему Диемитко. Пусть $\operatorname{ord} a$ — порядок a по модулю n. Условия 1) и 2) означают, что $q \mid \operatorname{ord} a$. В свою очередь $\operatorname{ord} a$ делит значение функции Эйлера $\varphi(n)$. Таким образом, $q \mid \varphi(n)$ и q либо совпадает с некоторым простым делителем p числа n, либо делит $p - 1$ (если $p^2 \mid n$). Первый случай невозможен, во втором случае $p = qr + 1$ и

$$n = (qr + 1)(qs + 1),$$

где r, s — четные, $r \geq 2$. Если n — составное, то $s \geq 2$ и, следовательно, $n \geq (2q + 1)^2$. Однако последнее условие нарушается при $R < 4(q + 1)$, и теорема Диемитко доказана.

Боб строит n так, что условия 1), 2) могут выполняться, хотя условие $R < 4(q+1)$ будет нарушено и n окажется составным. Конкретнее, составное n Боб получит, если

(a) $n = p^2$, где $p = 2q + 1$ — простое;

(b) n является k-битовым числом, а q — $[k/2]$-битовым (k должно быть нечетным);

(c) $\operatorname{ord} a = q$ или $\operatorname{ord} a = 2q$.

Например, $n = 121 = (2 \cdot 5 + 1)^2$ — минимальное число, удовлетворяющее первым двум требованиям.

Мультипликативная группа кольца вычетов по модулю $n = p^2 = (2q + 1)^2$ является циклической порядка $\varphi(n) = 2pq$. Пусть g — образующий этой группы. Тогда основания

$$a = g^{ip} \bmod n, \quad i = 1, 2, \ldots, q - 1, q + 1, \ldots, 2q - 1,$$

имеют порядок q или $2q$ и эти основания будут ошибочно свидетельствовать в пользу простоты составного n.

Например, для $n = 121$ и $q = 5$ ложными свидетелями будут $a \in \{3, 9, 27, 40, 81, 94, 112, 118\}$.

Обсуждение: ГОСТ Р 34.10-94. Алгоритм Боба с фиксированным основанием $a = 2$ используется в российском стандарте ГОСТ Р 34.10-94. С помощью этого алгоритма генерируются простые числа, которые применяются в алгоритмах электронной цифровой подписи.

Возникает вопрос: можно ли в ГОСТ Р 34.10-94 получить составное число? Составное n может привести к некорректной работе алгоритмов ЭЦП и вопрос актуален.

Обсуждение: Простые Жермен и простые Вифериха. [1] При доказательстве отдельных случаев последней теоремы Ферма А. Виферих и Софи Жермен ввели в рассмотрение специальные простые, впоследствии названные в их честь:

1. Простое q называется *простым Жермен*, если $p = 2q + 1$ — простое.
2. Простое p называется *простым Вифериха*, если $2^{p-1} \equiv 1 \pmod{p^2}$.

Простые Жермен достаточно часты, а вот простых Вифериха известно только два — это 1093 и 3511. Вычислительные эксперименты показывают, что других простых Вифериха вплоть до $1.25 \cdot 10^{15}$ нет. Тем не менее, считается (доказано при некоторых недоказанных предположениях), что таких простых бесконечно много.

Гипотеза. Если q — простое Жермен, то соответствующее $p = 2q + 1$ не может быть простым Вифериха.

Если гипотеза нарушается и $p = 2q+1$ — контрпример, то составное $n = p^2$ пройдет тест Боба с основанием 2. Но такое n, в принципе, может быть построено алгоритмом генерации простых ГОСТ Р 34.10-94!

Доказательство гипотезы для случая $q \equiv 3 \pmod 4$ объявлено в [Gallardo L. H. On special Wieferich's primes, arXiv:1002.3840, 2010, `http://arxiv.org/abs/1002.3840`]. Доказательство нами пока не проверено. В любом случае, полное доказательство гипотезы нам неизвестно.

[1] за обсуждение спасибо Д. Васильеву