Доказательство корректности и сертификат НОД

Еникеев Р.Р.

Казанский (Приволжский) федерельный университет

Введение

Пусть мы нашли $g = \text{НОД}(a, b)$. Каким образом можно проверить, что мы вычислили g корректно?

- Проверки условий $g|a$ и $g|b$ недостаточно
- Проверка, что все числа большие чем g не являются общими делителями a и b не эффективна
- Алгоритм Евклида работает корректно, но мы не можем быть уверены, что он правильно реализован.

Остается только вычислить НОД повторно.

Сертификат НОД — данные, с помощью которых можно проверить корректность найденного НОД быстрее, чем вычисляя его повторно.

Верификация — процесс проверки правильности НОД с помощью сертификата.

Сертификат

Актуальность

Сертификат может быть использован:

- Для проверки взаимной простоты двух чисел (частный случай при $g = 1$)
  - Для тестирования правильности сгенерированных ключей в алгоритме шифрования RSA (ключи должны быть взаимно простыми)
- Для проверки корректности НОД, полученного по сети или считанного из файла
- Для тестирования алгоритма вычисления НОД, который мы реализуем

Сертификат

Понятие «сертификат» используется:

- Определение класса NP
  - Проверка решения задачи с помощью сертификата/решения на ДМТ осуществляется за полиномиальное время
  - Сертификат для факторизации — искомое разложение
- Тест простоты Аткина–Морейна

Сохранение результатов итераций алгоритма Евклида

Данный метод:

- Похож на проверку простоты числа Аткина–Морейна (задача сводится к меньшей по размерности и сохраняется результат текущего этапа)
- Использует тот факт, что корректность алгоритма Евклида (АЕ) доказана
- Сертификат — результат работы каждой итерации АЕ:

$$a_i, b_i, \lfloor a_i / b_i \rfloor, a_i \bmod b_i$$

- Верификация — проверка того, что на каждой итерации вычисления производились правильно

Сохранение результатов итераций алгоритма Евклида

Создание сертификата

Algorithm 1 АЕ, возвращающий НОД и его сертификат

$CERTIFICATE := []$
while $b > 0$ **do**
  $(div, mod) := (\lfloor a/b \rfloor, a \bmod b)$
  $\text{Append}(CERTIFICATE, [a, b, div, mod])$
  $(a, b) := (b, mod)$
$g := a$
return $g, CERTIFICATE$

Сохранение результатов итераций алгоритма Евклида

Верификация с помощью сертификата

Algorithm 2 Верификация НОД с помощью сертификата

$n := Length(CERTIFICATE)$
$a_1, b_1, div_1, mod_1 := CERTIFICATE_1$
$a_n, b_n, div_n, mod_n := CERTIFICATE_n$
if $a \neq a_1$ **or** $b \neq b_1$ **or** $b_n \neq g$ **or** $mod_n \neq 0$ **then**
  return False
for $i := 1; i < n; i := i + 1$ **do**
  $a_i, b_i, div_i, mod_i := CERTIFICATE_i$
  $a_{i+1}, b_{i+1}, div_{i+1}, mod_{i+1} := CERTIFICATE_{i+1}$
  if $a_i! = b_i * div_i + mod_i$ **or** $a_{i+1} \neq b_i$ or $b_{i+1} \neq mod_i$ **then**
    return False
return True

Сохранение результатов итераций алгоритма Евклида

Свойства сертификата

Достоинства:

- Можно легко распараллелить верификацию
- Во время верификации используется умножение вместо вычисления остатка от деления

Недостатки:

- Количество памяти $O(N^2)$ (кол-во записей $O(N)$, длина чисел $O(N)$), где $N = \log b$

Коэффициенты Безу в качестве сертификата

Коэффициенты Безу

Пусть a и b целые числа, тогда существуют целые числа x и y (коэффициенты Безу) такие, что:

$$a * x + b * y = \text{НОД}(a, b).$$

Теорема. Пусть есть $x, y : a * x + b * y = g$ и выполняются условия $g|a$ и $g|b$, тогда $g = \text{НОД}(a, b)$.

Таким образом для доказательства правильности НОД нам достаточно вычислить коэффициенты Безу (создание сертификата) и показать, что выполняются условия из этой теоремы (верификация).

Для нахождения коэффициентов Безу мы используем расширенный алгоритм Евклида (РАЕ).

Коэффициенты Безу в качестве сертификата

Создание сертификата

Algorithm 3 PAE, возвращающий сертификат НОД

$(x_0, x_1, y_0, y_1) := (0, 1, 1, 0)$
while $b > 0$ **do**
  $q := \lfloor a/b \rfloor$
  $(a, b) := (b, a - q * b)$
  $(x_0, x_1) := (x_1, x_0 - q * x_1)$
  $(y_0, y_1) := (y_1, y_0 - q * y_1)$
$g := a$
$(a', b') := (a/g, b/g)$ {Чтобы во время верификации не было деления}
$CERTIFICATE := [x_0, y_0, a', b']$
return $g, CERTIFICATE$

Коэффициенты Безу в качестве сертификата

Свойства

Достоинства:

- Количество памяти $O(N)$, т. к. $|x| < \left|\frac{b}{g}\right|$ и $|y| < \left|\frac{a}{g}\right|$
- Верификация выполняется от 5 до 11 раз быстрее, чем повторное вычисление НОД.

Свойства сертификатов НОД

Достоинства всех методов, работающих с сертификатами:

- Сертификат достаточно сгенерировать только один раз, а верификацию с помощью одного и того же сертификата можно производить многократно.

Недостаток всех методов, работающих с сертификатами:

- Даже если проверяемый НОД является правильным, но сам сертификат содержит ошибку, тогда верификация даст ложноотрицательный результат.

Спасибо за внимание!