Практика №6. Алгоритм Евклида. Расширенный алгоритм Евклида. Тесты на простоту чисел. Генерация простых чисел.

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Алгоритм Евклида.

1. Ввод натуральных чисел a, b, a≥b.
2. Положить A=a и R=B=b.
3. Заменить значение R остатком от деления A на B и перейти к шагу 4.
4. Если R=0, то сообщить: «наибольший общий делитель равен B», и остановиться. В противном случае перейти к шагу 5.
5. Заменить значение A на значение B, Значение B на значение R и возвратиться к шагу 3.

Алгоритм отыскивает НОД двух положительных целых чисел a и b:

$a=b\,q_0+r_0 \qquad 0\le r_0<b$

$b=r_0\,q_1+r_1 \qquad 0\le r_i<r_{i+1}, \qquad i=1,\ldots,n$

$r_0=r_1\,q_2+r_2$

$\ldots\ldots\ldots$

$r_{n-1}=r_n\,q_{n+1}+r_{n+1}$

При $r_{n+1}=0$ $НОД(a,b)=r_n$

Выполняя обратную подстановку, НОД можно записать в виде $НОД(a,b)=xa+yb$.

Для программной реализации целесообразно использование алгоритма Кнута, в котором построена рекуррентная процедура:

$x_j = x_{j-2} - q_j x_{j-1},\ y_j = y_{j-2} - q_j y_{j-1}$

Необходимую информацию удобно свести в таблицу:

остатки	частные	x	y
a	*	x_{-1}	y_{-1}
b	*	x_0	y_0
r_1	q_1	x_1	y_1
…	…	…	…
r_{n-2}	q_{n-2}	x_{n-2}	y_{n-2}
r_{n-1}	q_{n-1}	x_{n-1}	y_{n-1}

Таким образом, для получения очередного значения x и y необходимо знание текущего остатка и двух предшествующих значений x и y.

Определение наибольшего общего делителя целых положительных чисел a и b позволяет найти наименьшее общее кратное этих чисел, используя теорему:

$НОД(a,b)\cdot НОК(a,b)=a\cdot b$

Решето Эратосфена.

Один из древнейших алгоритмов нахождения простых чисел. Начиная с 2, которое является первым простым числом, вычеркиваем все последующие числа, кратные 2. Следующее простое число 3, вычеркнем все числа после него, кратные 3. Таким образом, вычеркиваются все числа, делящиеся хотя бы на одно из простых чисел.

В компьютерных приложениях, требующих больших простых чисел обычно проверяют, не является ли случайно выбранное число простым с помощью подходящих критериев.

Одним из таких критериев служит метод выделения множителей Ферма: целое нечетное число n не является простым тогда и только тогда, когда существуют неотрицательные числа p и q, такие что $p^2-q^2=n$ и при этом $p-q>1$. Очевидно, если $p^2-q^2=n$, то $n=(p-q)(p+q)$, то есть n не простое число.

Применение этого метода заключается в попытке найти целые числа p и q, такие, что

- $p^2=n+q^2$. При это полагаем q=1, 2, 3,… до тех пор, пока $n+q^2$ не станет полным квадратом. Если до значения q=(n–1)/2 полный квадрат не будет достигнут, то n – простое число.

- $q^2=p^2–n$. При этом берем в качестве m наименьшее целое число такое, что $m^2 \geq n$, и последовательно полагаем p=m, m+1, … до тех пор, пока $p^2–n$ не станет полным квадратом. Так как q не может превысить значения (n–1)/2, то проверку продолжаем до значения p=(n+1)/2. Если полный квадрат не достигнут, значит n–простое число.

Для проверки простоты числа возможно использование вероятностных алгоритмов тестирования.

Тест Соловея- Штрассена.

1. Выберите случайное число a, меньшее p.
2. Если НОД(a,p)≠1, то число p не простое и не проходит тест.
3. Вычислите $j=a^{(p-1)/2} \bmod p$.
4. Вычислите символ Якоби J(a,p).
5. Если j≠J, то число p определенно не простое.
6. Если j=J(a,p), то вероятность того, что число p – простое не превышает 50%.

Тест Леманна.

1. Выберите случайное число a меньшее p.
2. Вычислите $a^{(p-1)/2} \bmod p$.
3. Если $a^{(p-1)/2} \bmod p \not\equiv 1$ или –1(mod p), то число определенно не простое.
4. Если $a^{(p-1)/2} \bmod p \equiv 1$ или –1(mod p), то вероятность того, что число p не простое не превышает 50%.
5. Повторите этот тест t раз. Если результат вычислений равен 1 или –1, но не всегда 1, то p – простое с вероятностью ошибки $1/2^t$.

Тест Рабина- Миллера.

1. Вычислите b – число делений p-1 на 2 и найдите m такое, что $p=1+2^b \cdot m$.
2. Выберите случайное число a, меньшее p.
3. Установите j=0 и $z=a^m \bmod p$.
4. Если z=1 или если z=p-1, то p проходит тест и может быть простым числом.
5. Если j>0 и z=1, то p не простое число.
6. Установите j=j+1. Если j<b и z≠p-1, установите $z=z^2 \bmod p$ и вернитесь на этап 5. Если z=p-1, то число проходит тест.
7. Если z=b и z≠p-1, то p не относится к простым числам.

Повторяйте проверку t раз с t различными значениями a для каждого числа p. Вероятность преодоления всех тестов составным числом p не превышает $1/2^t$, для тестов Соловея-Штрассена и Леманна, и $1/4^t$, для теста Рабина-Миллера.

Чем больше тестируемое число, тем больше предварительных вычислений рекомендуется произвести до вероятностного теста. Проверка делимости случайного числа на 3, 5, 7 отсекает 54% нечетных чисел; на все простые числа, меньшие 100 отбрасывает 76% нечетных чисел; на все простые числа, меньшие 256 исключает 80% нечетных чисел.

ЗАДАНИЯ

Напишите вспомогательную программу построения таблицы простых чисел меньших 256 с помощью решета Эратосфена.

Выясните с помощью метода Ферма, являются ли n произвольных чисел простыми; в случае составного числа разложите его на множители.

Для произвольного большого простого числа p выясните вопрос о его простоте:

- с помощью теста Соловея – Штрассена;
- с помощью теста Лемана;
- с помощью теста Рабина – Миллера;
- с помощью непосредственной проверки.