УДК 621.29

С.А. Инютин

Модулярные вычисления для задач большой алгоритмической сложности

(Сургутский государственный педагогический институт)

Вычисления с многоразрядными числами или вычисления с величинами, меняющимися в больших диапазонах, являются одной из областей, в которых модулярные вычислительные средства имеют преимущества перед иными, ориентированными на другие вычислительные базы. Важные для теории и практики математические задачи, требующие таких вычислений и больших вычислительных ресурсов, лежат в областях прикладной и вычислительной теории чисел [1]. Большинство таких задач (или проблем) содержат целочисленные вычисления с числами или числовыми величинами, принимающими значения из больших и сверхбольших машинных диапазонов. В настоящее время интенсивно развивается прикладная теория чисел, отвечая потребности в надежной передаче, хранении и обработке коммерческой и иной цифровой информации. Возникает широкий спектр вычислительных задач [2,7], приводящих к вычислениям, при которых значения целочисленных переменных значительно, в 10^3,…10^6 и более раз превышают максимум типового компьютерного диапазона серийной вычислительной техники, определяемого длиной аппаратно-поддерживаемого ма-

шинного слова. Назовём такой диапазон большим целочисленным компьютерным диапазоном. Наличие эффективных методов вычислений в больших диапазонах позволяет ставить задачи вычислений в сверхбольших диапазонах, максимум которых достигает значения константы Виноградова - Гольбаха $3^{3^{15}}$.

Перечислим ряд задач, часто называемых из-за их сложности вычислительными проблемами [2].

1. Тестирования на простоту чисел специального вида.
2. Тестирования на простоту чисел произвольного вида.
3. Вычисление простых делителей и нахождение канонического мультипликативного разложения числа.
4. Поиск больших и сверхбольших простых чисел вида $4 \cdot k+1$.
5. Поиск псевдопростых чисел.
6. Поиск чисел близнецов.
7. Поиск нечетного совершенного числа.
8. Поиск цепочек простых чисел в арифметических прогрессиях.
9. Проверка местоположения нулей дзета-функции Римана.

Данный перечень не является исчерпывающим. Характерной особенностью указанных в нем задач является невозможность их решения в настоящее время только аналитическими или алгебраическими методами, и по этой причине находят широкое использование вычислительные методы при поиске полного или частичного решения, контрпримеров. На некоторые из этих проблем современная точка зрения такова, что найти их удовлетворительные решения возможно только вычислительными методами. Решения перечисленных задач имеют большое теоретическое значение. На данный момент даже частные решения, полученные вычислительными методами, отдельных из указанных вычислительных проблем, находят, наряду с теоретическим, также широкое практическое приложение. Соотношение между их теоретической значимостью и практической ценностью постоянно меняется [3,10].

При классификации методов вычислений в больших и сверхбольших компьютерных диапазонах необходимо учитывать наряду с постановкой исходной задачи особенности модулярных вычислительных процессов.

Задачи вычислений в сверхбольших компьютерных диапазонах (СБД) определены ранее. Введём классификацию методов вычислений в СБД, взяв в качестве типовых методы, возникающие при решении задач тестирования на простоту чисел специального вида: Ферма и Мерсенна.

Кодонезависимые варианты алгоритмов тестирования имеют близкий вид [8].

Algorithm Pepen.

1. $m \neg 0$, $A \neg 3$
2. $A \neg A^2 (\mathrm{mod}\ F_n)$, $m \neg m+1$
3. *if* $2^n - m = 0$ *then end else goto 2*
4. *end: if* $A = 2^{2^n}$ *then* F_n*- prime else* F_n*–not prime*

Algorithm Lucas-Lehmer.

1. $m \neg 0$, $A \neg 4$
2. $A \neg A^2 - 2 (\mathrm{mod}\ M_n)$, $m \neg m+1$
3. *if* $m = n-2$ *then end else goto 2*
4. *end: if* $u \circ 0 (\mathrm{mod}\ M_n)$ *then* M_n*- prime else* M_n*–not prime*

Базовой операцией этих методов является вычисление вычета от некоторой сверхбольшой величины по модулю, являющемуся большой величиной. Каноническое разложение большого модуля F_n или M_n , как правило, неизвестно. Возможно, что большой модуль является простым.

$$C = | A^{f(B)} |_B = A^{f(B)} - N \cdot B \ ,$$

где $A, B, f(B)$ - большие числовые величины;

$A^{f(B)}$ - сверхбольшая числовая величина.

Так как $A^{f(B)}$ -сверхбольшая числовая величина, то прямые алгоритмы, базирующиеся на вычислении соотношения:

$$C = A^{f(B)} - [A^{f(B)} / B] \cdot B \ ,$$

невозможно или нецелесообразно реализовать на вычислительной технике из- за большой алгоритмической и временной сложности.

Модулярная арифметика МС(P^2) позволяет рассматривать это равенство в форме сравнения по модулю $P^2 > C$:

$$C(\mathrm{mod}\, P^2) \equiv$$
$$(A^{f(B)}(\mathrm{mod}\, P^2) - [A^{f(B)} / B](\mathrm{mod}\, P^2) \cdot B(\mathrm{mod}\, P^2))(\mathrm{mod}\, P^2)$$

При таком подходе возможны два способа итерационного вычисления большой величины $C(mod\ P^2)$.

Определение. Вычетным итерационным алгоритмом 1 -рода называется алгоритм, который вычисляют при $B<P^2$, в частности при $B<P$, большую величину $C(mod\ P^2)$:

$$C(\mathrm{mod}\, P^2) = \mid A^{f(B)} \mid_B (\mathrm{mod}\, P^2) \ ,$$

как последовательность:

$$C(\mathrm{mod}\, P^2) = \mid ... \parallel A^{f_1(B)} \mid_B^{f_2(B)} \mid_B ... \mid_B (\mathrm{mod}\, P^2) \ ,$$

при этом предполагается выполнение соотношения, характеризующего мультипликативную структуру показателя степени, например заданного каноническим мультипликативным разложением:

$$f(B) = f_1(B) \cdot f_2(B) ..... \quad .$$

Определение. Вычетным итерационным алгоритмом 2 -рода называется алгоритм, который вычисляет при $B<P^2$ сверхбольшую величину $N(mod\ P^2)$, а затем большую величину

$$C(mod\ P^2) :$$

$$N(\mathrm{mod}\ P^2) =$$

$$[A^{f(B)} / B](\mathrm{mod}\ P^2) = ((A^{f(B)} - X_i(\mathrm{mod}\ P^2)) \cdot \backslash B \backslash^{-1})(\mathrm{mod}\ P^2)^{,}$$

где последовательность больших величин X_i , оцениваемая некоторым образом, стремится к $C(mod\ P^2)$.

Отличие между алгоритмами 1 ,2 -родов заключается в том, что для модулярного алгоритма 2- рода в МС(P^2) целая величина $N(mod\ P^2\ )$, вычисляемая методом формального деления в МС(P^2), должна совпасть с целой величиной N , полученной фактическим делением на B .

Среди итерационных вычетных алгоритмов 1,2 -родов целесообразно выделение подкласса алгоритмов, основанных на оценивании интервала, в котором может находиться сверхбольшая величина.

Например, для F_n n - числа Ферма выполняются неравенства:

$$2^{f(F_n)} < 3^{f(F_n)} < 4^{f(F_n)} \quad .$$

Если при таком оценивании границы вычисляются с меньшей алгоритмической сложностью и их разность меньше значения большой величины - P^2 , то возможно вычисление соответствующего вычета как алгебраической суммы вычета от значения границы и некоторой фиксированной разницы искомой сверхбольшой величины и границы интервала оценивания:

$$|3^{f(F_n)}|_B = \| 2^{f(F_n)}|_B + |\Delta|_B|_B \ (\mathrm{mod}\, P^2) \quad .$$

Это позволяет ввести следующие определения.

Определение. Алгоритм называется вычетным итерационным оценочным алгоритмом 1 –рода, если вычисляет большую величину $C(mod\ P^2)$ как алгебраическую сумму по модулю B в МС(P^2) некоторой сверхбольшой величины R и разности искомой сверхбольшой величины и R :

$$C = |R|_B + |R - A^{f(B)}|_B - 0\,|B(mod\ P^2\ ) \quad .$$

Определение. Алгоритм называется вычетным итерационным оценочным алгоритмом 2 –рода, если вычисляет сверхбольшую величину:

$$N = [A^{f(B)} / B]$$

как алгебраическую сумму в МС(P^2) некоторой сверхбольшой величины M и разности искомой сверхбольшой величины N и M по модулю P^2, что позволяет большую величину C вычислять в соответствии с соотношением:

$$C(\mathrm{mod}\, P^2) = (A^{f(B)}(\mathrm{mod}\, P^2) - (M(\mathrm{mod}\, P^2) - (N - M)(\mathrm{mod}\, P^2)) \cdot B)(\mathrm{mod}\, P^2) .$$

При разработке способов преобразования проблемных алгоритмов в вычетную форму, ориентированную на модулярную арифметику и соответствующую вычислительную базу, необходимо учесть следующие моменты [4,5,6].

Пусть вычислительная задача заключается в получении для содержательной, математически - корректно постановленной проблемы из некоторой области результатов численных расчетов для переменных, изменяющихся в сверхбольших диапазонах. При множестве преобразований вычислительного алгоритма должна сохраняться или заменяться на эквивалентную исходная постановка проблемы. Конечные численные или на их основе качественные результаты должны быть инвариантны к способу получения. На промежуточных этапах вычислительного процесса инвариантность результатов вычислений не требуется. Следовательно, алгоритм вычислительного процесса может быть преобразован в другую, например, «вычетную форму». Даже, если при преобразованиях на этом уровне теряется эквивалентность постановок более высокого уровня, всё равно такие преобразования возможны на этом уровне, если при этом сохраняется эквивалентность в постановке проблемы на ещё более высоком уровне абстракции. Процесс преобразований может быть продолжен, его естественным пределом является необходимость сохранения инвариантности конечных результатов к методу их получения.

ЛИТЕРАТУРА

1. *Рибенбойм П.* Рекорды простых чисел. // Успехи математических наук. Т. 42, вып. 5, 1987. -С.119-176.

2. *Lenstra H.W. , Tijdeman R..J.* Computational Methods in Number Theory. –Amsterdam: Math. Cent., 1982. –198p.

3. *Ноден П. и др.* Алгебраическая алгоритмика. –М.: Мир, 1999. – 720с.

4. *Амербаев В.М.* Теоретические основы машинной арифметики. -Алма-Ата: Наука, 1976. -320 с.

5. *Инютин С.А.* Основы многоразрядной алгоритмики. -Сургут: РИО, 2002. -137с.

6. *Inyutin S.A.* Parallel Square Modular Computer Algebra // Lecture Notes in Computer Science: Parallel Processing and Applied Mathematics (PPAM). – German -Poland: Springer, 2003, -LNCS № 3019. –p. 993-997.

7. *Инютин С.А.* Модулярные вычисления в сверхбольших компьютерных диапазонах // Известия вузов. Электроника. -2001, -№ 6. –с. 34-39.

8. *Инютин С.А.* Помехозащитные модулярные кодовые конструкции квадратичного диапазона // Вестник Тюменского госуниверситета. –Тюмень: -2003, - № 5. –с. 173-180.

9. *Инютин С.А.* Компьютерная модулярная алгебра квадратичного диапазона и область ее приложения // Вестник Тюменского госуниверситета. –Тюмень: -2001, - № 2. –с. 141-148.

10. *Инютин С.А.* Вычислительные задачи большой алгоритмической сложности и модулярная арифметика // Вестник Тюменского госуниверситета. –Тюмень: -2002, - № 3. –с. 3-9.