Алгебра и теория чисел

Иван Казменко

Кружок обучения мастерству программирования при мат-мехе СПбГУ

Четверг, 4 октября 2012 года

Оглавление

Работа с остатками по модулю

Постановка задачи: нужно производить арифметические действия над целыми числами по модулю m.

- **Лемма 1:** $(a \pm b) \bmod m = ((a \bmod m) \pm (b \bmod m)) \bmod m$.
- **Лемма 2:** $(a \cdot b) \bmod m = ((a \bmod m) \cdot (b \bmod m)) \bmod m$.
- Для деления такое равенство неверно.

Работа с остатками по модулю

Постановка задачи: нужно производить арифметические действия над целыми числами по модулю m.

- **Лемма 1:** $(a \pm b) \bmod m = ((a \bmod m) \pm (b \bmod m)) \bmod m$.
- **Лемма 2:** $(a \cdot b) \bmod m = ((a \bmod m) \cdot (b \bmod m)) \bmod m$.
- Для деления такое равенство неверно.

Работа с остатками по модулю

Постановка задачи: нужно производить арифметические действия над целыми числами по модулю m.

- **Лемма 1:** $(a \pm b) \bmod m = ((a \bmod m) \pm (b \bmod m)) \bmod m$.
- **Лемма 2:** $(a \cdot b) \bmod m = ((a \bmod m) \cdot (b \bmod m)) \bmod m$.
- Для деления такое равенство неверно.

Работа с остатками по модулю

Постановка задачи: нужно производить арифметические действия над целыми числами по модулю m.

- **Лемма 1:** $(a \pm b) \bmod m = ((a \bmod m) \pm (b \bmod m)) \bmod m$.
- **Лемма 2:** $(a \cdot b) \bmod m = ((a \bmod m) \cdot (b \bmod m)) \bmod m$.
- Для деления такое равенство неверно.

«Медленное» умножение

Постановка задачи: вычисление $(a \cdot b) \bmod m$.

«Медленное» умножение

Постановка задачи: вычисление $(a \cdot b) \bmod m$.
Если числа порядка m^2 помещаются в тип данных, можно просто применить Лемму 1: $(a \cdot b) \bmod m = ((a \bmod m) \cdot (b \bmod m)) \bmod m$.

«Медленное» умножение

Постановка задачи: вычисление $(a \cdot b) \bmod m$.
Если же число m^2 слишком велико, можно произвести умножение «в столбик» в двоичной записи:

- Вычислим $a \bmod m$, $2a \bmod m$, $4a \bmod m$, $8a \bmod m$, ...
- Рассмотрим двоичную запись b и просуммируем нужные слагаемые с предыдущего шага, после каждого сложения вычисляя остаток по модулю m.
- **Пример:** $a = 13$, $b = 10$, $m = 21$.
  $b = 10_{10} = 1010_2 = 2 + 8$
  $(1 \cdot a) \bmod m = 13$
  $(2 \cdot a) \bmod m = (13 + 13) \bmod 21 = 26 \bmod 21 = 5$
  $(4 \cdot a) \bmod m = (5 + 5) \bmod 21 = 10$
  $(8 \cdot a) \bmod m = (10 + 10) \bmod 21 = 20$
  Ответ: $(((2 \cdot a) \bmod m) + ((8 \cdot a) \bmod m)) \bmod m =$
  $(5 + 20) \bmod m = 25 \bmod 21 = 4$.

«Медленное» умножение

Постановка задачи: вычисление $(a \cdot b) \bmod m$.
Если же число m^2 слишком велико, можно произвести умножение «в столбик» в двоичной записи:

- Вычислим $a \bmod m$, $2a \bmod m$, $4a \bmod m$, $8a \bmod m$, ...
- Рассмотрим двоичную запись b и просуммируем нужные слагаемые с предыдущего шага, после каждого сложения вычисляя остаток по модулю m.
- **Пример:** $a = 13$, $b = 10$, $m = 21$.
  $b = 10_{10} = 1010_2 = 2 + 8$
  $(1 \cdot a) \bmod m = 13$
  $(2 \cdot a) \bmod m = (13 + 13) \bmod 21 = 26 \bmod 21 = 5$
  $(4 \cdot a) \bmod m = (5 + 5) \bmod 21 = 10$
  $(8 \cdot a) \bmod m = (10 + 10) \bmod 21 = 20$
  Ответ: $(((2 \cdot a) \bmod m) + ((8 \cdot a) \bmod m)) \bmod m =$
  $(5 + 20) \bmod m = 25 \bmod 21 = 4$.

«Медленное» умножение

Постановка задачи: вычисление $(a \cdot b) \bmod m$.
Если же число m^2 слишком велико, можно произвести умножение «в столбик» в двоичной записи:

- Вычислим $a \bmod m$, $2a \bmod m$, $4a \bmod m$, $8a \bmod m$, ...
- Рассмотрим двоичную запись b и просуммируем нужные слагаемые с предыдущего шага, после каждого сложения вычисляя остаток по модулю m.
- **Пример:** $a = 13$, $b = 10$, $m = 21$.
  $b = 10_{10} = 1010_2 = 2 + 8$
  $(1 \cdot a) \bmod m = 13$
  $(2 \cdot a) \bmod m = (13 + 13) \bmod 21 = 26 \bmod 21 = 5$
  $(4 \cdot a) \bmod m = (5 + 5) \bmod 21 = 10$
  $(8 \cdot a) \bmod m = (10 + 10) \bmod 21 = 20$
  Ответ: $(((2 \cdot a) \bmod m) + ((8 \cdot a) \bmod m)) \bmod m =$
  $(5 + 20) \bmod m = 25 \bmod 21 = 4$.

«Медленное» умножение

Постановка задачи: вычисление $(a \cdot b) \bmod m$.
Если же число m^2 слишком велико, можно произвести умножение «в столбик» в двоичной записи:

- Вычислим $a \bmod m$, $2a \bmod m$, $4a \bmod m$, $8a \bmod m$, $\ldots$.
- Рассмотрим двоичную запись b и просуммируем нужные слагаемые с предыдущего шага, после каждого сложения вычисляя остаток по модулю m.
- **Пример:** $a = 13$, $b = 10$, $m = 21$.
  $b = 10_{10} = 1010_2 = 2 + 8$
  $(1 \cdot a) \bmod m = 13$
  $(2 \cdot a) \bmod m = (13 + 13) \bmod 21 = 26 \bmod 21 = 5$
  $(4 \cdot a) \bmod m = (5 + 5) \bmod 21 = 10$
  $(8 \cdot a) \bmod m = (10 + 10) \bmod 21 = 20$
  Ответ: $(((2 \cdot a) \bmod m) + ((8 \cdot a) \bmod m)) \bmod m =$
  $(5 + 20) \bmod m = 25 \bmod 21 = 4$.

«Медленное» умножение

Постановка задачи: вычисление $(a \cdot b) \bmod m$.
Если же число m^2 слишком велико, можно произвести умножение «в столбик» в двоичной записи:

- **Пример:** $a = 13,\ b = 10,\ m = 21.$
  $b = 10_{10} = 1010_2 = 2 + 8$
  $(1 \cdot a) \bmod m = 13$
  $(2 \cdot a) \bmod m = (13 + 13) \bmod 21 = 26 \bmod 21 = 5$
  $(4 \cdot a) \bmod m = (5 + 5) \bmod 21 = 10$
  $(8 \cdot a) \bmod m = (10 + 10) \bmod 21 = 20$
  Ответ: $(((2 \cdot a) \bmod m) + ((8 \cdot a) \bmod m)) \bmod m =$
  $(5 + 20) \bmod m = 25 \bmod 21 = 4.$
- **Проверка:** $(13 \cdot 10) \bmod 21 = 130 \bmod 21 = (126 + 4) \bmod 21 = 4.$
- Заметим, что при вычислениях могут получиться только числа от 0 до $2 \cdot m - 2$.

«Медленное» умножение

Постановка задачи: вычисление $(a \cdot b) \bmod m$.
Если же число m^2 слишком велико, можно произвести умножение «в столбик» в двоичной записи:

- **Пример:** $a = 13$, $b = 10$, $m = 21$.
  $b = 10_{10} = 1010_2 = 2 + 8$
  $(1 \cdot a) \bmod m = 13$
  $(2 \cdot a) \bmod m = (13 + 13) \bmod 21 = 26 \bmod 21 = 5$
  $(4 \cdot a) \bmod m = (5 + 5) \bmod 21 = 10$
  $(8 \cdot a) \bmod m = (10 + 10) \bmod 21 = 20$
  Ответ: $(((2 \cdot a) \bmod m) + ((8 \cdot a) \bmod m)) \bmod m =$
  $(5 + 20) \bmod m = 25 \bmod 21 = 4$.
- **Проверка:** $(13 \cdot 10) \bmod 21 = 130 \bmod 21 = (126 + 4) \bmod 21 = 4$.
- Заметим, что при вычислениях могут получиться только числа от 0 до $2 \cdot m - 2$.

«Медленное» умножение

Постановка задачи: вычисление $(a \cdot b) \bmod m$.
Если же число m^2 слишком велико, можно произвести умножение «в столбик» в двоичной записи:

- Вычислим $a \bmod m$, $2a \bmod m$, $4a \bmod m$, $8a \bmod m$, ...
- Рассмотрим двоичную запись b и просуммируем нужные слагаемые с предыдущего шага, после каждого сложения вычисляя остаток по модулю m.
- **Время работы:** $\log_2 b$ сложений по модулю для вычисления $(2^k \cdot a) \bmod m$ и не более $\log_2 b$ сложений по модулю для суммирования нужных слагаемых.

«Быстрое» возведение в степень

Постановка задачи: вычисление $a^b \bmod m$.

«Быстрое» возведение в степень

Постановка задачи: вычисление $a^b \bmod m$.
Будем действовать аналогично: умножение можно представить как последовательность сложений, а возведение в степень — как последовательность умножений.

- Вычислим $a \bmod m$, $a^2 \bmod m$, $a^4 \bmod m$, $a^8 \bmod m$, ...
- Рассмотрим двоичную запись b и вычислим произведение нужных множителей с предыдущего шага, после каждого умножения вычисляя остаток по модулю m.

«Быстрое» возведение в степень

Постановка задачи: вычисление $a^b \bmod m$.
Будем действовать аналогично: умножение можно представить как последовательность сложений, а возведение в степень — как последовательность умножений.

- Вычислим $a \bmod m$, $a^2 \bmod m$, $a^4 \bmod m$, $a^8 \bmod m$, ...
- Рассмотрим двоичную запись b и вычислим произведение нужных множителей с предыдущего шага, после каждого умножения вычисляя остаток по модулю m.
- **Пример:** $a = 13$, $b = 5$, $m = 21$.
  $b = 5_{10} = 101_2 = 1 + 4$
  $a^1 \bmod m = 13$
  $a^2 \bmod m = (13 \cdot 13) \bmod 21 = 169 \bmod 21 = 1$
  $a^4 \bmod m = (1 \cdot 1) \bmod 21 = 1$
  Ответ: $((a^1 \bmod m) \cdot (a^4 \bmod m)) \bmod m = (13 \cdot 1) \bmod m = 13$.

«Быстрое» возведение в степень

Постановка задачи: вычисление $a^b \bmod m$.
Будем действовать аналогично: умножение можно представить как последовательность сложений, а возведение в степень — как последовательность умножений.

- Вычислим $a \bmod m$, $a^2 \bmod m$, $a^4 \bmod m$, $a^8 \bmod m$, ….
- Рассмотрим двоичную запись b и вычислим произведение нужных множителей с предыдущего шага, после каждого умножения вычисляя остаток по модулю m.
- **Пример:** $a = 13$, $b = 5$, $m = 21$.
  $b = 5_{10} = 101_2 = 1 + 4$
  $a^1 \bmod m = 13$
  $a^2 \bmod m = (13 \cdot 13) \bmod 21 = 169 \bmod 21 = 1$
  $a^4 \bmod m = (1 \cdot 1) \bmod 21 = 1$
  Ответ: $((a^1 \bmod m) \cdot (a^4 \bmod m)) \bmod m = (13 \cdot 1) \bmod m = 13$.

«Быстрое» возведение в степень

Постановка задачи: вычисление $a^b \bmod m$.
Будем действовать аналогично: умножение можно представить как последовательность сложений, а возведение в степень — как последовательность умножений.

- Вычислим $a \bmod m$, $a^2 \bmod m$, $a^4 \bmod m$, $a^8 \bmod m$, $\ldots$.
- Рассмотрим двоичную запись b и вычислим произведение нужных множителей с предыдущего шага, после каждого умножения вычисляя остаток по модулю m.
- **Пример:** $a = 13$, $b = 5$, $m = 21$.
  $b = 5_{10} = 101_2 = 1 + 4$
  $a^1 \bmod m = 13$
  $a^2 \bmod m = (13 \cdot 13) \bmod 21 = 169 \bmod 21 = 1$
  $a^4 \bmod m = (1 \cdot 1) \bmod 21 = 1$
  Ответ: $((a^1 \bmod m) \cdot (a^4 \bmod m)) \bmod m = (13 \cdot 1) \bmod m = 13$.

«Быстрое» возведение в степень

Постановка задачи: вычисление $a^b \bmod m$.
Будем действовать аналогично: умножение можно представить как последовательность сложений, а возведение в степень — как последовательность умножений.

- **Пример:** $a = 13,\ b = 5,\ m = 21.$
  $b = 5_{10} = 101_2 = 1 + 4$
  $a^1 \bmod m = 13$
  $a^2 \bmod m = (13 \cdot 13) \bmod 21 = 169 \bmod 21 = 1$
  $a^4 \bmod m = (1 \cdot 1) \bmod 21 = 1$
  Ответ: $((a^1 \bmod m) \cdot (a^4 \bmod m)) \bmod m = (13 \cdot 1) \bmod m = 13.$
- **Проверка:** $(13^5) \bmod 21 = 371\,293 \bmod 21 = 13.$
- Заметим, что при вычислениях могут получиться только числа от 0 до $(m-1)^2$.
- Если умножения по модулю реализовать при помощи «медленного» умножения, при вычислениях могут вновь получиться только числа от 0 до $2 \cdot m - 2$.

«Быстрое» возведение в степень

Постановка задачи: вычисление $a^b \bmod m$.
Будем действовать аналогично: умножение можно представить как последовательность сложений, а возведение в степень — как последовательность умножений.

- **Пример:** $a = 13$, $b = 5$, $m = 21$.
  $b = 5_{10} = 101_2 = 1 + 4$
  $a^1 \bmod m = 13$
  $a^2 \bmod m = (13 \cdot 13) \bmod 21 = 169 \bmod 21 = 1$
  $a^4 \bmod m = (1 \cdot 1) \bmod 21 = 1$
  Ответ: $((a^1 \bmod m) \cdot (a^4 \bmod m)) \bmod m = (13 \cdot 1) \bmod m = 13$.
- **Проверка:** $(13^5) \bmod 21 = 371\,293 \bmod 21 = 13$.
- Заметим, что при вычислениях могут получиться только числа от 0 до $(m-1)^2$.
- Если умножения по модулю реализовать при помощи «медленного» умножения, при вычислениях могут вновь получиться только числа от 0 до $2 \cdot m - 2$.

«Быстрое» возведение в степень

Постановка задачи: вычисление $a^b \bmod m$.
Будем действовать аналогично: умножение можно представить как последовательность сложений, а возведение в степень — как последовательность умножений.

- **Пример:** $a = 13$, $b = 5$, $m = 21$.
  $b = 5_{10} = 101_2 = 1 + 4$
  $a^1 \bmod m = 13$
  $a^2 \bmod m = (13 \cdot 13) \bmod 21 = 169 \bmod 21 = 1$
  $a^4 \bmod m = (1 \cdot 1) \bmod 21 = 1$
  Ответ: $((a^1 \bmod m) \cdot (a^4 \bmod m)) \bmod m = (13 \cdot 1) \bmod m = 13$.
- **Проверка:** $(13^5) \bmod 21 = 371\,293 \bmod 21 = 13$.
- Заметим, что при вычислениях могут получиться только числа от 0 до $(m-1)^2$.
- Если умножения по модулю реализовать при помощи «медленного» умножения, при вычислениях могут вновь получиться только числа от 0 до $2 \cdot m - 2$.

«Быстрое» возведение в степень

Постановка задачи: вычисление $a^b \bmod m$.
Будем действовать аналогично: умножение можно представить как последовательность сложений, а возведение в степень — как последовательность умножений.

- Вычислим $a \bmod m$, $a^2 \bmod m$, $a^4 \bmod m$, $a^8 \bmod m$, ...
- Рассмотрим двоичную запись b и вычислим произведение нужных множителей с предыдущего шага, после каждого умножения вычисляя остаток по модулю m.
- **Время работы:** $\log_2 b$ умножений по модулю для вычисления $a^{2^k} \bmod m$ и не более $\log_2 b$ умножений по модулю для перемножения нужных сомножителей.

Всё.