http://aafin.ru/m/rsaa.html

Содержание

1 Вычисления в кольце вычетов

Как известно, обычные числа — это такая линеечка с делениями. В обычных числах есть первичная операция «плюс один», или «на одно деление вправо», и вторичные — сложение, умножение и возведение в степень. Вторичные они потому, что сложение это многократное «плюс один», умножение — многократное сложение, и возведение в степень — многократное умножение.

Обычные числа — это очень просто, и поэтому для нужд криптографии изобрели «ненормальные числа», в которых всё сложно.

Ненормальные числа — это такой «циферблатик», т.е. линеечка, загнутая в кольцо.

Пример 1. На обыкновенных часах со стрелкой 12 делений, таким образом получается 12 чисел. Ненормальные криптографы нумеруют их так: 0, 1, 2, . . . , 11. (А не 1, 2, . . . , 12, как все нормальные люди).

Этот «циферблатик» называется кольцо вычетов с 12 числами или Z_{12}. Размеры «циферблатика» могут быть разными, т.е. существует много разных систем ненормальных чисел.

1.1 Сложение и умножение

Арифметические операции с ненормальными числами в принципе такие же, но первичная операция «плюс один» зацикливается, т.е. 11 «плюс один» будет 0. Операции сложения, умножения и возведения в степень определяются аналогично обычным числам.

Пример 2. 10 + 5=пять раз «плюс один» после десяти. Считаем пальчиком по циферблатику: 11, 0, 1, 2, 3. Получается $10 + 5 = 3$ в ненормальных числах Z_{12}.

Пример 3. 10^3 это $10 \cdot 10 \cdot 10$. В свою очередь $10 \cdot 10$ это $10 + 10 + 10 + 10 + 10 + 10 + 10 + 10 + 10 + 10$. И в свою очередь $10 + 10$ это (считаем пальчиком) 11, 0, 1, 2, 3, 4, 5, 6, 7, 8. Т.е. $10 + 10 = 8$. Продолжая считать пальчиком, когда-нибудь найдем 10^3.

Эти же действия можно сделать с помощью калькулятора. Представим себе обыкновенные числа в виде верёвочки с узелками, а циферблат в виде бревна с обхватом «12 узелков». Теперь вычислять можно так: сначала отсчитываем узелки на верёвке, затем наматываем её на бревно и смотрим, какой хвостик остался.

Пример 4. 10^3 можно сосчитать на калькуляторе, получится 1000 (т.е веревочка, на которой тысяча узелков). Наматываем: 1000 поделить на 12 (можно на калькуляторе) будет 83 с мелочью, т.е. 83 полных оборота и хвостик. 83 полных оборота по 12 узелков будет 996, т.е. на хвостик остается 4 узелка. Вот мы и сосчитали, $10^3 = 4$ в ненормальных числах Z_{12}.

Кстати, то, что мы только что проделали, называется деление с остатком. (см. раздел 2.1 (стр. 5)). В равенстве $1000=12\cdot 83+4$ число 1000 — делимое, 12 — делитель, 83 — частное и 4 — остаток. Если пользоваться обозначениями из популярных языков программирования, то 1000%12=4.

1.2 Вычитание

Напомним, что вычитание — это операция, обратная к сложению, т.е. $a - b = c$ это то же самое, что и $a = c + b$.

Немногие знают, что «черточка» в математике обозначает три разных вещи:

1. Вычитание, т.е операция, обратная к сложению.
2. Часть числа. Обычных чисел иногда не хватает, и люди придумали расширение — отрицательные числа. К сожалению, бедные на фантазию математики обозначают их посредством пририсовывания черточки перед числом.
3. Операцию взятия противоположного числа. Напомним, что два числа называются *противоположными*, если их сумма равна 0. Как известно, $3 + (-3) = 0$, и это значит, что 3 противоположно -3 и -3 противоположно 3.

Присмотревшись к калькулятору с кнопочками, можно обнаружить там три «минуса»: один справа в середине, второй обычно внизу слева, и третий появляется на индикаторе при появлении там отрицательного числа.

В ненормальных числах всё немного не так. Противоположные числа там уже есть изначально, так что пририсовывать черточку к числу не нужно: $7+5=0$ в Z_{12} т.е. 7 — число противоположное к 5, а 5 — число противоположное к 7.

значное двоичное и, следовательно, для возведения в стозначную степень нужно сделать не более 800 умножений. Почти любой компьютер с этим легко справится.

1.5 Извлечение корня

В обычных числах корень извлекают методом половинного деления[2]. Поскольку в кольце вычетов слова «одно число правее другого» не имеют смысла, то и метод половинного деления не работает. Есть ли другие методы извлечения корня (кроме тупого перебора, конечно)?

Это сложный вопрос, ответ на который пока не найден. Но в некоторых специальных случаях такой алгоритм существует, и про него вы сейчас прочитаете.

Напомним, что число называется *простым*, если оно ни на что не делится (кроме 1 и самого себя). Так вот, если в кольце вычетов количество чисел простое число (Z_2, Z_3, Z_5, Z_7, ...), то у такого кольца вычетов появляются некоторые приятные свойства. Например, у всех чисел (кроме 0) есть обратное (см. раздел 1.3.1 (стр. 2)), если произведение двух чисел равно 0, то одно из них 0 (но в Z_6, как показано в примере 8 (стр. 2), это не так), и еще кое что. Но нас будет интересовать

Утверждение 1 (Малая теорема Ферма)**.** *Если p простое число, то в Z_p, для всех чисел x из Z_p (кроме 0), выполнено равенство*

$$x^{(p-1)} = 1.$$

Пример 10. В Z_3 выполняется: $1^2 = 1$, $2^2 = 4 = 3 + 1 = 1$.

В Z_5 выполняется: $1^4 = 1$, $2^4 = 16 = 15 + 1 = 1$, $3^4 = (3^2)^2 = 4^2 = 1$, $4^4 = (4^2)^2 = 1^2 = 1$.

Но в Z_4 не выполняется: $2^3 = 8 = 0$, $3^3 = 9 \cdot 3 = 1 \cdot 3 = 3$.

Благодаря этому самому Ферма, у нас есть

1.5.1 Алгоритм извлечения корня в в Z_p, если p простое

Он работает в два шага: предположим, некто дал нам задание найти $\sqrt[\alpha]{a} = x$ в Z_p.

1. Найдем обратное к степени (т.е. к α) в Z_{p-1} (внимание, там написано на единицу меньше). Если обратного нет, то это значит, что этот алгоритм применять нельзя. Так этому Некту и говорим и идем отдыхать. Но если обратное всё-таки есть, придется переходить к шагу два.

2. Итак, мы нашли обратное т.е. $\beta \cdot \alpha = 1$ в Z_{p-1}. Теперь, вместо извлечения корня степени α, мы будем возводить a в степень β. (Внимание, вычисления проводятся опять в исходном кольце вычетов Z_p). Следующее предложение весьма важно, и поэтому мы поместим его в рамочку:

   $$\boxed{\text{Оказывается, } a^\beta = x \text{ в } Z_p.}$$

   Напоминаем, что у нас есть (см. раздел 1.4) быстрый алгоритм возведения в степень, его и следует применять.

Пример 11. Найдем $\sqrt[3]{4}$ в Z_{11}.

1. Найдем 3^{-1} в Z_{10} так, как это сделано в разделе 1.3 (стр. 2). Если вы всё сделаете правильно, то у вас получится $3^{-1} = 7$. Проверим на всякий случай: $3 \cdot 7 = 21 = 10 \cdot 2 + 1$.

2. Возводим 4 в седьмую степень в Z_{11}: $4^7 = (4^2 \cdot 4)^2 \cdot 4 = (16 \cdot 4)^2 \cdot 4 = (5 \cdot 4)^2 \cdot 4 = 20^2 \cdot 4 = 9^2 \cdot 4 = 81 \cdot 4 = 4 \cdot 4 = 16 = 5$

Итак, ответ $\sqrt[3]{4} = 5$ в Z_{11}.

Сделаем проверку: $5^3 = 5 \cdot 5 \cdot 5 = 25 \cdot 5 = 3 \cdot 5 = 15 = 4$.

Разоблачение фокуса: нам нужно, чтобы $x^\alpha = a$ в Z_p. У нас $\beta \cdot \alpha = 1$ в Z_{p-1}, на обычном языке это означает, что остаток от деления равен 1, т.е. выполнение равенства $\beta \cdot \alpha = (p-1) \cdot t + 1$. Итак: $x^\alpha = (a^\beta)^\alpha = a^{\beta \cdot \alpha} = a^{(p-1) \cdot t + 1} = (a^{(p-1)})^t \cdot a^1$. И, по малой теореме Ферма (утв. 1 (стр. 3)), $a^{(p-1)} = 1$ в Z_p, и всё доказано.

Упражнение 3. Убедитесь, что в Z_{12} этот алгоритм не работает (и не должен, 12 не простое число).

Кстати, из теоремы 1 (стр. 3) следует

Утверждение 2 (Про возведение в степень и $p-1$)**.** *Если два числа (a и b) отличаются друг от друга на $p-1$ (т.е. $a = b + \alpha \cdot (p-1)$), то в Z_p (p — простое число) возведение в степень a и возведение в степень b это одно и то же.*

Действительно, так как $x^{p-1} = 1$, выполняется равенство: $x^a = x^{b + \alpha \cdot (p-1)} = x^b \cdot (x^{p-1})^\alpha = x^b \cdot 1^\alpha = x^b$.

Упражнение 4. Найдите $2^{22222222222222222222222}$ в Z_{11}. Можно ли это вычислить без калькулятора и перерывов на сон и еду?

1.6 Китайская теорема об остатках и извлечение корня

Кроме нормальных чисел (в виде линеечки с делениями) и ненормальных колец вычетов (в виде циферблатика), существует еще более хитрое вычислительное устройство в виде «велосипедика»[3].

Представьте себе две звездочки, соединенные цепью примерно как у велосипеда. Их вращение синхронизировано так, что поворот на один зубчик одной звездочки приводит к повороту на один зубчик другой звездочки. На зубцах звездочек написаны числа совсем как у кольца вычетов. Звездочки на заводе установлены в положение $(0, 0)$, т.е. левая звездочка в положении 0 и правая тоже в положении 0.

Операция «плюс один» в этом «велосипедике» — это поворот обеих звездочек на один зубчик. Если делать «плюс один» несколько раз, то положение звездочек будет меняться: $(1, 1)$, $(2, 2)$, ... Дальше всё зависит от размеров звездочек, если они одинакового размера, то ничего интересного происходить не будет, получится обычное кольцо вычетов в двух экземплярах. Но если их размеры разные, то получится примерно так:

Пример 12. Пусть, для примера, на левой звездочке три зубца, а на правой четыре. Тогда положения звездочек будут меняться так: $0 - (0, 0)$, $1 - (1, 1)$, $2 - (2, 2)$, $3 - (0, 3)$, $4 - (1, 0)$, $5 - (2, 1)$, $6 - (0, 2)$, $7 - (1, 3)$, $8 - (2, 0)$, $9 - (0, 1)$, $10 - (1, 2)$, $11 - (2, 3)$. И потом опять $(0, 0)$, $(1, 1)$, ...

Присмотревшись, можно заметить, что звездочки проходят через все возможные комбинации в странном порядке и потом возвращаются в исходное положение. Оказывается верно

[2] Погуглите, чтоб узнать. goo.gl/Iut1et

[3] Не пугайтесь, по-научному это называется *прямое произведение колец вычетов*

Если его умножить на -6

$$11 \cdot (1 \cdot (-6)) + 5 \cdot (-2 \cdot (-6)) = 1 \cdot (-6),$$

то получится как раз равенство (2)

$$11 \cdot (-6) + 5 \cdot (12) = -6.$$

Упс. Не получается. α и β получились отрицательными. Плохо. Что же делать?

Придумал! Нужно попробовать другое соотношение Безу, с другими знаками. (Как его найти, написано в утверждении 6 (стр. 6)).

$$11 \cdot (-4) + 5 \cdot (9) = 1.$$

Умножаем на -6

$$11 \cdot (24) + 5 \cdot (-54) = -6.$$

и сравниваем с формулой 2. Вот мы и нашли, $\alpha = 24$, $\beta = 54$. Подставив $\alpha = 24$ в верхнее уравнение (1), найдем $x=11 \cdot 24+9=273$. Подставив $\beta=54$ в нижнее уравнение (1), найдем $x = 5 \cdot 54 + 3 = 273$. Совпадает, это хорошо. Более того, $273 = 55 \cdot 4 + 53 = 53$ в Z_{55}, совсем как в примере 15 (стр. 4).

Упражнение 5. Убедитесь, не заглядывая в таблицу, что в примере 15 паре $(4, 2)$ действительно соответствует число 37.

1.7 RSA, Эль–Гамаль и миллионер, но социалист

Погуглив эту абракадабру, вы погрузитесь в загадочный мир современной криптографии, и с удивлением обнаружите, что вам почти всё понятно!

Секретный ключ в RSA — это два простых числа (достаточно больших, стозначных например), публичный ключ — это их произведение, шифрование — это возведение сообщения в степень (обычно в третью) в кольце вычетов, а дешифрование — это извлечение корня, про которое вы только что прочитали в разделе 1.6.

И даже загадочные «Схема Эль–Гамаля» и задача миллионера–социалиста[5] покажутся не такими уж и непонятными после чтения раздела 1.3.1 (стр. 2) про обратные числа и 1.4.1 (стр. 2) про быстрое возведение в степень.

2 Теория чисел

Из этой главы вы узнаете кое-что про целые числа. Напомним, что целые числа это $\ldots, -3, -2, -1, 0, 1, 2, 3, 4, \ldots$, и их можно представлять себе как очень очень длинную линеечку с делениями. На этих числах есть первичная операция «плюс один» или «на одно деление вправо», и вторичные — сложение, умножение и возведение в степень. Вторичные они потому, что сложение это многократное «плюс один», умножение — многократное сложение, и возведение в степень — многократное умножение. Кроме этого, у вышеперечисленных операций есть обратные: вычитание, деление и извлечение корня, впрочем, всё это вы, вероятно, проходили в школе.

[5] «Socialist millionaires», на русский язык эту статью в Википеди пока никто не соизволил перевести.

goo.gl/1aIOhg

2.1 Деление с остатком

Деление с остатком проходят в школе. Напомним, что равенство вида

$$A = B \cdot C + R$$

называется делением числа A на число B с остатком. Точнее, A — делимое, B — делитель, C — частное и R — остаток. Остаток (т.е. R) должен быть меньше частного (т.е. B), иначе нещитово.

Это равенство можно представлять себе как наматывание веревочки длиной A на бревно с обхватом B. Получится C полных оборотов и «хвостик» R.

Пример 17. Если веревочку длиной 7 наматывать на бревно с обхватом 3, то получится два полных оборота и «хвостик» длины 1. Это можно записать формулой $7=3 \cdot 2+1$, или сказать, что остаток от деления 7 на 3 равен 1.

В дальнейшем, нам особенно часто придется находить остаток от деления, и поэтому мы будем пользоваться обозначением из популярного языка программирования: $A\%B = R$.

При нахождении остатка от деления на обыкновенном калькуляторе приходится записывать целую часть частного на бумажку и потом вводить обратно в калькулятор. И это неудобно. Но зато проверку можно делать не отрывая рук от калькулятора:

Упражнение 6. Докажите, что для проверки равенства $A\%B = R$ достаточно вычислить $(A - R)/B$. Если получается целое число, то всё в порядке, если не целое, то не в порядке.

Упражнение 7. Определите, какое из равенств верно, ничего не записывая на бумажку: $1234\%567 = 100$ или $1234\%567 = 101$?

2.2 Наибольший общий делитель и соотношение Безу

Будем говорить, что одно число *делится* на другое, если оно делится нацело, т.е. без остатка. Например, 12 делится на 4 $(12/4 = 3)$ и не делится на 5 $(12/5 = 2.4)$. То число, на которое делится другое число, называется *делителем*. Например, 4 делитель 12, но 5 не делитель 12.

Наибольший общий делитель (НОД) — это наибольшее число, являющееся общим делителем (Капитан Очевидность одобряет это определение).

Пример 18. Число 12 делится на 1, 2, 3, 4, 6 и 12. Число 8 делится на 1, 2, 4 и 8. Таким образом, НОД$(12, 8) = 4$.

Если НОД двух чисел равен 1, то говорят, что они *взаимно просты*.

Поиск НОД тупым перебором возможен у маленьких чисел и невозможен у больших. (Про это написано в разделе 3.2 (стр. 7)). Более того, поскольку при нахождении НОД нужно искать «самое большое из возможных», то возникает «проблема плохого начальника», (про него написано в разделе 3.1 (стр. 7)), которую, в данном случае, можно решить с помощью соотношения Безу, и сейчас вы узнаете, как это сделать.

Утверждение 5. *Оказывается, если* НОД$(A, B) = N$, *то можно найти пару целых чисел* u, v *(одно из них отрицательное) таких, что*

$$A \cdot u + B \cdot v = N.$$

Это равенство и называется соотношение Безу.

В программировании, эта цепочка подчиненных называется *стек вызова функции.*

Вероятно, у вас на контрольной не будет под рукой подчинённого, и поэтому вам самому придется быть своим подчинённым, давать задания самому себе, а стек вызова писать на бумажке в столбик.

Пример 23. Найдем числа в равенстве Безу для 29 и 12. Производя деления с остатком ($29 = 12 \cdot 2 + 5$, $12 = 5 \cdot 2 + 2$), построим стек:

$$\begin{aligned} 29 \cdot (\quad) + 12 \cdot (\quad) &= \\ 12 \cdot (\quad) + 5 \cdot (\quad) &= \\ 5 \cdot (\quad) + 2 \cdot (\quad) &= \end{aligned}$$

Числа 5 и 2 достаточно маленькие, и понятно, что их НОД равен 1, и соотношение Безу получится такое:

$$5 \cdot (-1) + 2 \cdot (3) = 1$$

Начнем заполнять стек снизу вверх. Первый шаг:

$$\begin{aligned} 29 \cdot (\quad) + 12 \cdot (\quad) &= 1 \\ 12 \cdot (\quad) + 5 \cdot (\quad) &= 1 \\ 5 \cdot (-1) + 2 \cdot (3) &= 1 \end{aligned}$$

По формуле (3 (стр. 6)) найдем соотношение Безу для 12 и 5:

$$12 \cdot (3) + 5 \cdot (-7) = 1$$

и заполним следующую строчку в стеке:

$$\begin{aligned} 29 \cdot (\quad) + 12 \cdot (\quad) &= 1 \\ 12 \cdot (3) + 5 \cdot (-7) &= 1 \\ 5 \cdot (-1) + 2 \cdot (3) &= 1 \end{aligned}$$

И, аналогично, еще одну строчку:

$$\begin{aligned} 29 \cdot (-7) + 12 \cdot (17) &= 1 \\ 12 \cdot (3) + 5 \cdot (-7) &= 1 \\ 5 \cdot (-1) + 2 \cdot (3) &= 1 \end{aligned}$$

Итак, соотношение Безу найдено: $29 \cdot (-7) + 12 \cdot (17) = 1$.

(Читерская подсказка: заметили, как число из второй скобки переползает в первую строчкой выше? Ну так это не случайность, а формула (3 (стр. 6)). И число во второй скобке можно находить, просто решая уравнение с одной переменной).

Если мы собираемся производить вычисления со стозначными числами, то неплохо бы заранее прикинуть размеры этого стека. Погуглив Википедию, можно узнать, что в алгоритме Евклида за два шага числа уменьшаются примерно в два раза, т.е для стозначных чисел понадобится примерно 800 подчиненных.

3 Всякая всячина

Тут будет то, что по какой-либо причине не поместилось в предыдущие главы.

3.1 Проблема плохого начальника

Предположим, начальник задал вам математическую задачу. Вы её решали, решали и решили. Принесли решение начальнику, а он и говорит: «Чем докажешь, что решал? Может ты просто число какое-то наугад написал и теперь денег моих хочешь?»

И тогда вы медленно, по пунктам показываете этому нехорошему человеку, как именно вы решали. А он медленно и занудно на калькуляторе проверяет все вычисления а потом и говорит: «А за что деньги-то платить? Все эти вычисления я сам только что проделал своими собственными руками, лучше я сам себе заплачу».

В некоторых случаях проблема разрешима. Например, если задали «решать квадратное уравнение через дискриминант», вы можете торжественно сказать «**Чтобы проверить, надо подставить!**». Потом радостно, на глазах начальника подставить корни в уравнение и доказать, что ответ правильный. Конечно, нехороший начальник вычтет из зарплаты стоимость трёх умножений и двух сложений, но остальные деньги (после вычета налогов), наверное, отдаст.

Отсюда мораль: недостаточно уметь находить правильный ответ, нужно ещё уметь находить легко проверяемое *доказательство правильности ответа.*

3.2 Невозможное вычисление

Как известно, компьютеры стали более лучше ~~одеваться~~ вычислять и почти достигли гиперзвука. Олимпиард операций в наносекунду скоро уже не предел. Есть ли такие задачи, которые компьютеры никогда вычислять не смогут?

Предположим, наш супер процессор настолько быстр, что совершает одну операцию за время прохождения светом расстояния, равного радиусу атома (10^{-19} секунд). Предположим, мы никуда не торопимся, и 13.7 миллиардов ($1.37 \cdot 10^{10}$) лет машинного времени (это возраст Вселенной) нас не пугают.

Один год это $60 \cdot 60 \cdot 24 \cdot 365 = 31536000 \approx 3 \cdot 10^7$ секунд. Простые вычисления показывают, что даже в этом случае больше $4.3 \cdot 10^{36}$ операций не сделать.

И даже если сделать сверх многопроцессорный сверх компьютер с $1.3 \cdot 10^{50}$ процессорами (столько атомов в земном шаре), за гугол (10^{100}) операций всё равно не вылезти. Так что, если для решения задачи требуется гугол операций, можно расслабиться и ничего не делать.

Упражнение 8. Сколько тысяч миллиардов возрастов Вселенных понадобится этому сверх многопроцессорному сверх компьютеру для подбора стозначного пароля состоящего только из цифр?

Ответы на упражнения

Упр. 1. Ответ: $x = 4$. Проверка: $4 + 3 = 7 = 5 + 2 = 2$.
Упр. 2. Ответ: $x = 39$. Проверка: $33 \cdot 39 + 25 = 1312 = 32 \cdot 41 + 0 = 0$.
Упр. 4. Ответ: Можно. Получится 4.
Упр. 8. Ответ: Не меньше тысячи.

Предметный указатель