Семинар 9.
Теория чисел и числовые алгоритмы

Составил Р. Делла Пиетра

25.4.20

1 Базовые факты

Работаем с вычетами по некоторому модулю, то есть остатками от деления $\mathbb{Z}$ на некоторое число m, что обозначается как $\mathbb{Z}/m\mathbb{Z}$ или $\mathbb{Z}_m$. По сути это значит, что целые числа разбиваются на m классов эквивалентности, и к примеру $7 = 17m+7 \mod m$, то есть эти два разных целых числа лежат в одном классе эквивалентности. Разных классов, очевидно, m: $\{0, 1, \ldots, m-1\}$.

$(a, m) = 1 \implies$ если x пробегает все возможные вычеты по модулю m, $ax + b$ также пробегает все вычеты.
Приведённые вычеты — взаимно простые с m.
$(a, m) = 1 \implies$ если x пробегает все приведённые вычеты по модулю m, ax также пробегает все приведённые вычеты.

1.1 Функция Эйлера

Вспомним про φm — функцию Эйлера. $\varphi m=$ количество чисел, меньших m и взаимно простых с ним. Некоторые очевидные свойства: если m простое, $\varphi(m) = m - 1$.
$(a, b) = 1, m = ab \implies \varphi(m) = \varphi(a)\varphi(b)$.
$\varphi(p^\alpha) = p^\alpha(1 - \frac{1}{p})$ для простого p.
$m = \prod p_i^{\alpha_i} \implies \varphi(m) = \prod \varphi p_i^{\alpha_i} = \prod p_i^{\alpha_i}(1 - \frac{1}{p_i}) = m \prod(1 - \frac{1}{p_i})$

1.2 Теорема Лагранжа

$(a, m) = 1 \implies a^{\varphi m} = 1 \mod m$.
Доказательство: возьмём приведённую систему вычетов $\{b_1, \ldots, b_{\varphi(m)}\}$ по модулю m. По одному из свойств выше $\{ab_1, \ldots, ab_{\varphi(m)}\}$ также будет приведённой системой вычетов, но, возможно, в другом порядке.
Тогда $\prod\limits_{k=1}^{\varphi(m)} b_k = \prod\limits_{k=1}^{\varphi(m)} ab_k \mod m$, то есть $a^{\varphi(m)} = 1 \mod m$.
Частный случай этой теоремы: $m = p$ — простое число, тогда теорема превращается
в малую теорему Ферма: $a^{p-1} = 1 \mod m$.

1.3 Китайская теорема об остатках

Форма 1: пусть нам даны $\{m_1, \ldots, m_k\}$ — взаимно простые модули и $\{a_1, \ldots, a_k\}$ — некоторые остатки, каждый в соответствующем модуле. Тогда у системы $x = a_i \mod m_i \ \forall i$ есть одно решение
по модулю $M = \prod m_i$, равное такой величине:

$$x = \sum a_i \frac{M}{m_i} \left(\left(\frac{M}{m_1} \right)^{-1} \mod m_i \right)$$

Форма 2: $M = \prod\limits^{k} m_i$, $(m_i, m_j) = 1 \implies \mathbb{Z}/M\mathbb{Z} = \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$

1.4 Найти $119^{47^{250}} \mod 91$

Воспользуемся КТО: $91 = 13 \cdot 7$, поэтому будем искать остатки отдельно по 13 и по 7.
$A = 119^{47^{250}} \mod 7 = 0$, потому что 119 делится на 7.
$B = 119^{47^{250}} \mod 13$. $119 = 2 \mod 13 \implies B = 2^{47^{250}} \mod 13$.
По малой теореме Ферма $2^{12} = 1 \mod 13 \implies 2^{\alpha} = 2^{\alpha \mod 12} \mod 13$.
$47^250 = (-1)^250 = 1 \mod 12 \implies B = 2 \mod 13$.
Снова по КТО собираем ответ: $x = 0 \cdot \frac{91}{7}((\frac{91}{7})^{-1} \mod 7) + 2 \cdot \frac{91}{13}((\frac{91}{13})^{-1} \mod 13) = 14 \cdot (7^{-1} \mod 13)$.
Для того, чтобы найти $a = 7^{-1}$, воспользуемся алгоритмом Евклида: $7a + 13b = 1$.
$\begin{pmatrix} 13 & 7 \\ 6 & 7 \\ & 1 \end{pmatrix} \implies 1 = 7 - 6 = 7 - (13 - 7) = 2 \cdot 7 - 13 \implies 2 = 7^{-1} \mod 13$.
В итоге ответ $14 \cdot 2 = 28 \mod 91$.

2 Квадратичные вычеты

Кроме приведённых вычетов, можно ещё ввести понятие квадратичных вычетов: такие остатки, для которых уравнение $x^2 = a \mod m$ имеет решение.
У таких уравнений всегда 0 или 2 решения для простых модулей больше 2 (не учитывая $a = 0$): если $x^2 = a$, то $(-x)^2 = a$, и для простого p $x \neq -x \mod p$. Таким образом, все ненулевые вычеты делятся на пары с одинаковыми квадратами, то есть квадратичных вычетов в два раза меньше, чем обычных ненулевых вычетов. Таким образом, для простого p система вычетов состоит из нуля, $\frac{p-1}{2}$ квадратичных вычетов и столько же квадратичных невычетов. Далее в этом разделе слово «квадратичные» будет опускаться.

2.1 Свойства

Свойство квадратичности вычета относительно произведения работает как знак + или − у чисел:
произведение вычетов вычет, произведение невычетов вычет, а вычета и невычета невычет.
Также если a (не)вычет, то a^{-1} тоже: $aa^{-1} = 1$, а 1 всегда вычет.

2.2 Символы Лагранжа и Якоби

Введём индикатор квадратичности вычета:

$$a^{\frac{p-1}{2}} = \begin{cases} a\text{-вычет} \implies a^{\frac{p-1}{2}} = (b^2)^{\frac{p-1}{2}} = b^{p-1} = 1 \\ \hline a\text{-невычет} \implies \begin{array}{c} \text{возьмём все вычеты } \{r_i\}: \\ a^{\frac{p-1}{2}} = \prod r_i \prod \frac{a}{r_i} = (p-1)! = -1 \mod p \\ \text{слева произведение всех вычетов и невычетов, то есть все ненулевые вычеты} \\ \text{второе — теорема Вильсона} \end{array} \end{cases}$$

Таким образом, введём обозначение $\left(\frac{a}{m}\right) = a^{\frac{p-1}{2}} = 1$ если вычет, -1 иначе.
Свойства:
1) $a = a_1 \mod p \implies \left(\frac{a}{p}\right) = \left(\frac{a_1}{p}\right)$
2) $\left(\frac{1}{p}\right) = 1$
3) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$
4) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
5) $\left(\frac{\prod a_i}{p}\right) = \prod \left(\frac{a_i}{p}\right) \implies \left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$

Также введём расширение символа Лежандра — символ Якоби: $P = \prod p_i \implies \left(\frac{1}{P}\right) = \prod \left(\frac{1}{p_i}\right)$, где p_i простые, возможно с повторами. Для символа Якоби действуют те же свойства, и ещё квадратичный закон взаимности: если P и Q взаимно простые и нечётные,
6) $\left(\frac{P}{Q}\right) = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}} \left(\frac{Q}{P}\right)$.

2.3 Есть ли решения уравнения $x^2 = 219 \mod 383$?

Для этого надо найти $\left(\frac{219}{383}\right)$.
$\left(\frac{219}{383}\right) =_6 -\left(\frac{383}{219}\right) =_1 -\left(\frac{164}{219}\right) =_5 -\left(\frac{4}{219}\right)\left(\frac{41}{219}\right) =_{5,2} -\left(\frac{41}{219}\right) =_6 -\left(\frac{219}{41}\right) =_1 -\left(\frac{14}{41}\right) =_5 -\left(\frac{2}{41}\right)\left(\frac{7}{41}\right) =_3$
$-\left(\frac{7}{41}\right) =_6 -\left(\frac{41}{7}\right) =_1 -\left(\frac{-1}{7}\right) =_2 1$.
Получили 1, то есть 219 квадратичный вычет, поэтому решения для этого уравнения есть.

2.4 Найти остаток от деления числа Фибоначчи номер k на p

$k = \underbrace{2008^{2008^{2008^{\cdots}}}}_{2008 \text{ раз}}$
$p = 17$
Для начала решим в общем случае, дальше для данных чисел.
Вспомним формулу Бине: $F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$.
Рассмотрим два случая: если 5 квадратичный вычет по модулю p, то находим $\sqrt{5}$, поставляем в уравнение и находим $F_k \mod p$ как любую другую формулу используя свойства вычетов и сравнений по модулю.
Если 5 невычет по модулю p, всё усложняется. Многочлен $x^2 - 5$ неприводим в $\mathbb{Z}_p[x]$, поэтому по нему можно факторизовать, и рассматривать вычеты не просто в виде чисел от 0 до p, а вычеты — многочлены степени не более 1 и коэффициентами из $\mathbb{Z}_p$. Такая конструкция называется алгебраическим расширением поля, и также реализована для комплексных чисел: многочлен $i^2 + 1$ от переменной i неприводим на $\mathbb{R}$, поэтому рассматриваются многочлены степени не более 1, и составляют они привычное $\mathbb{C}$. Операции с многочленами в таком алгебраическом расширении работают так: как только встречаем x^2, заменяем на 5 (i^2 на -1), и снова остаёмся среди тех же остатков степени не более 1.
Таким образом, пришли к такой формуле: $F_n = \frac{x}{5}\left(\left(\frac{1+x}{2}\right)^n - \left(\frac{1-x}{2}\right)^n\right)$.
Теперь считаем для наших чисел: посчитав обратные по модулю 17, получим такую формулу:
$F_n = 7x((9+9x)^n - (9-9x)^n)$.
Дальше требуется соображение такого вида: ненулевые многочлены из $\mathbb{Z}_p[x]/(x^2+5)$, которых $17^2 - 1 = 288$, образуют конечное поле. Это значит, что мультипликативная группа этого поля, то есть поле без нуля (обозначается как $(\mathbb{Z}_p[x]/(x^2+5))^\times$), циклична, то есть существует генератор — элемент, который в порождает все остальные своими разными степенями.
Всего элементов 288, поэтому, если генератор g, $g^{289} = g$, или $g^{288} = 1$.
$\forall(ax+b)\ \exists t : g^t = ax + b \implies (ax+b)^{288} = g^{288t} = 1^t = 1$.
Таким образом, ищем $k \mod 288$. Включая КТО, получаем, что это $k = 64 \mod 288$.
$F_k = 7x((9+9x)^{64} + (9-9x)^{64})$.
Считаем $(9 \pm 9x)^{64}$ пошаговым возведением в квадрат, получаем $(-2 \mp 2x)$.
Подставляя, получаем $F_k = 7x(-4x) = -120 = 13 \mod 17$.

3 Простые числа лежат в $\mathcal{NP}$

Соберём факты, которые мы уже знаем:

- $p \in \mathbb{P} \implies a^{p-1} = 1 \mod p$
- $(\mathbb{Z}_p)^\times$ — циклическая группа, у неё есть генератор
- Если x генератор, то $\forall k < p-1 \quad x^k \neq 1 \mod p$

Пусть $r \in (\mathbb{Z}_p)^\times$. Это число не генератор, если $\exists t < p-1 : \ r^t = 1 \mod p$.
$r = x^a \implies r^t = x^{at} = x^{p-1} \implies t$ делит $p-1$. Таким образом, для проверки того, что число — генератор, достаточно проверить $x^{\frac{p-1}{p_i}} \neq 1 \mod p$ для всех p_i-делителей $p-1$.
Если p составное число, то группа не циклична, генератор не найдётся.
Таким образом, можно построить алгоритм на НМТ:

- Отгадываем генератор x
- Отгадываем разложение $p-1$ на простые множители $\{p_i\}$
- Проверяем, что генератор действительно генератор: $x^{p-1} = 1 \mod p$, $x^{\frac{p-1}{p_i}} \neq 1 \mod p$
- Рекурсивно проверяем, что p_i действительно простые числа

На сертификатное определение $\mathcal{NP}$ алгоритм распространяется таким образом: сертификатом будет генератор, разложение $p-1$ на простые множители и рекурсивно сертификаты для множителей $p-1$.
Можно показать, что и длина сертифаката, и количество операций ограничиваются логарифмом n в некоторой константной степени.