Не сделано
Спросим
Делается
Криво сделано
Сделано

Определения

Граф, матрица смежности, матрица инциденции, изоморфизм графов, автоморфизм графов, гомеоморфизм графов, гомотопическая эквивалентность графов, род графа (цикломатическое число), путь, числа реберной и вершинной связности, валентность вершины, дерево, остовное дерево, поток, мощность потока, градиент функции, заданной на вершинах графа, разрез, транспортная сеть, двудольный граф, паросочетание, совершенное паросочетание, планарный граф, кольцо, поле, изоморфизм колец, мультипликативная группа кольца, неприводимый многочлен, отображение Фробениуса.

Алгоритмы

1. Алгоритм нахождения кратчайшего пути в графе (два варианта).
2. Жадный алгоритм нахождения остовного дерева максимального веса.
3. Алгоритм Форда-Фалкерсона.
4. Венгерский алгоритм.
5. Алгоритм нахождения оптимального назначения.

Вычисления в конечных полях *(ТР 9)*

1. проверка неприводимости многочлена над конечным полем;
2. перечисление неприводимых многочленов малых степеней над малыми конечными полями;
3. построение конечного поля из p^n элементов;
4. нахождение порядка заданного элемента (по умножению).

Теоремы

1. Корректность алгоритма нахождения кратчайшего пути в графе.
2. Корректность жадного алгоритма.
3. Корректность алгоритма Форда-Фалкерсона.
4. Корректность венгерского алгоритма.
5. Корректность алгоритма нахождения оптимального назначения.
6. Формула для рода графа.
7. Связный граф без циклов имеет род 0 и наоборот. (Равносильность двух определений дерева.) Связь между числом вершин и ребер дерева.
8. Связь между числами реберной и вершинной связности.
9. Критерий эйлеровости графа.
10. Множество потоков является линейным пространством, размерность которого равна роду графа.
11. Множество градиентов является линейным пространством, размерность которого на единицу меньше числа вершин.
12. Базис пространства потоков, связанный с остовным деревом.
13. Поток в траспортной сети. Определение мощности потока.
14. Сумма значений потока в транспортной сети на ребрах любого разреза равна мощности

потока.
15. Теорема Форда-Фалкерсона.
16. Теорема Менгера (реберная).
17. Теорема Холла.
18. Критерий двудольности графа (теорема Кенига).
19. Теорема Эйлера о планарных графах.
20. Непланарность V_5.
21. Непланарность $V_{3,3}$.
22. Теорема Понтрягина-Куратовского (б/д).
23. Опеределение характеристики поля. Любое конечное поле содержит простое подполе $\mathbf{F}_p$.
24. Теорема о делении многочленов с остатком. Теорема Безу.
25. Многочлен степени n над полем имеет не более n корней. Пример многочлена над кольцом, имеющего больше корней, чем его степень.
26. Теорема о разрешимости диофантова уравнения в кольце многочленов над полем: если многочлена $A(t)$ и $B(t)$ не имеют общих множителей, то существуют такие многочлены $X(t)$ и $Y(t)$, что $A(t)X(t) + B(t)Y(t) = 1$.
27. Теорема об однозначности разложения многочлена над полем на неприводимые множители. Пример многочлена над кольцом, для которого это не так.
28. Пусть $\mathbf{K}$ поле, дан многочлен ненулевой степени $P(t) \in \mathbf{K}[\,t\,]$. Конструкция фактор-кольца $\mathbf{L} = \mathbf{K}[\,t\,]/(P(t))$. Доказательство того, что $\mathbf{L}$ поле тогда и только тогда, когда многочлен $P(t)$ неприводим.
29. Пусть $\mathbf{K}$ поле, дан неприводимый многочлен ненулевой степени $P(t) \in \mathbf{K}[\,t\,]$. Конструкция фактор-кольца $\mathbf{L} = \mathbf{K}[\,t\,]/(P(t))$. Доказательство того, что $\mathbf{L}$ поле тогда и только тогда, когда многочлен $P(t)$ имеет корень в $\mathbf{L}$.
30. Конечное поле характеристики p содержит p^n элементов.
31. Любой ненулевой элемент конечного поля из p^n элементов удовлетворяет уравнению $x^{p^n-1}-1 = 0$.
32. Отображение Фробениуса $\Phi(x) = x^p$. Его свойства.
33. Пусть неприводимый многочлен $P(t) \in \mathbf{F}_p[\,t\,]$ степени n имеет в поле $\mathbf{F}_{p^n}$ корень α. Тогда $P(t)$ имеет в $\mathbf{F}_{p^n}$ ровно n различных корней.
34. Конечная подгруппа мультипликативной группы поля циклическая.
35. Многочлен 2 и 3 степени неприводим, если он не имеет корней. Пример приводимого многочлена более высокой степени, не имеющего корней.

Определения

Граф, матрица смежности, матрица инциденции, изоморфизм графов, автоморфизм графов, гомеоморфизм графов, гомотопическая эквивалентность графов, род графа (цикломатическое число), путь, числа реберной и вершинной связности, валентность вершины, дерево, остовное дерево, поток, мощность потока, градиент функции, заданной на вершинах графа, разрез, транспортная сеть, двудольный граф, паросочетание, совершенное паросочетание, планарный граф, кольцо, поле, изоморфизм колец, мультипликативная группа кольца, неприводимый многочлен, отображение Фробениуса.

Граф — это совокупность не пустого множества вершин и наборов пар вершин (связей между вершинами).

Матрица смежности графа *G* с конечным числом вершин *n* (пронумерованных числами от 1 до *n*) — это квадратная матрица *A* размера *n*×*n*, в которой значение элемента a_{ij} равно числу рёбер из *i*-й вершины графа в *j*-ю вершину.

Иногда, особенно в случае неориентированного графа, петля (ребро из *i*-й вершины в саму себя) считается за два ребра, то есть значение диагонального элемента a_{ii} в этом случае равно удвоенному числу петель вокруг *i*-й вершины.

Матрица смежности простого графа (не содержащего петель и кратных ребер) является бинарной матрицей и содержит нули на главной диагонали.

Матрица инциденции — это матрица, значения элементов которой характеризуется инцидентностью (т.е. если v_1, v_2 — вершины, а $e = (v_1, v_2)$ — соединяющее их ребро, тогда вершина v_1 и ребро e инцидентны, вершина v_2 и ребро e тоже инцидентны) соответствующих вершин графа (по вертикали) и его рёбер (по горизонтали). Для неориентированного графа элемент принимает значение 1, если соответствующие ему вершина и ребро инцидентны. Для ориентированного графа элемент принимает значение 1, если инцидентная вершина является началом ребра, значение -1, если инцидентная вершина является концом ребра; в остальных случаях (в том числе и для петель) значению элемента присваивается 0.

Изоморфизм. Два графа называются изоморфными, если существует перестановка вершин, при которой они совпадают. Иначе говоря, два графа называются изоморфными, если существует взаимно-однозначное соответствие между их вершинами и рёбрами, которое сохраняет смежность и инцидентность (графы отличаются только названиями своих вершин).
Точное определение: Изоморфизмом графов $G = \langle V_G, E_G \rangle$ и $H = \langle V_H, E_H \rangle$ называется биекция между множествами вершин графов $f\colon\ V_G \to V_H$ такая, что любые две вершины u и v графа G смежны тогда и только тогда, когда вершины $f(u)$ и $f(v)$ смежны в графе H. В случае, если понятие изоморфизма применяется к ориентированным или взвешенным графам, накладываются дополнительные ограничения на сохранение ориентации дуг и значений весов. Если изоморфизм графов установлен, они называются изоморфными и обозначаются как $G \simeq H$.

Автоморфизм графов — изоморфизм графов с самими собой.

Гомеоморфизм графов. Графы G1, G2 называются гомеоморфными, если существуют их подразбиения, являющиеся изоморфными.
Подразделением ребра (v_1,v_2) графа называется операция добавления в граф вершины v' и замены этого ребра на два смежных ребра (v_1,v') и (v',v_2): V'=V+{v'}, E'=E-{(v_1,v_2)}+{(v_1,v')}+{(v',v_2)}.

Гомотопическая эквивалентность графов. Два графа называются *гомотопически*

эквивалентными, если из одного из них можно получить другой путем стягивания вершин графа.

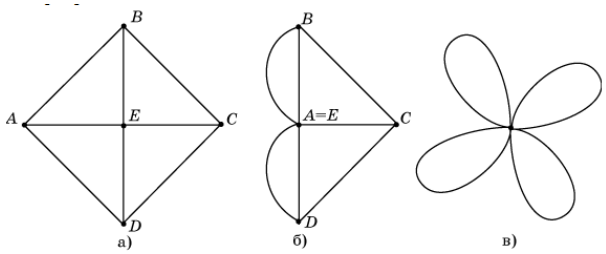


Рис. 8

Пример стягивания вершин:

Род графа (цикломатическое число):

1. g = P - B + 1, где P - число ребер, B - число вершин.

2. Наименьшее число ребер, которое надо удалить, чтобы получилось дерево.

3. Кол-во окружностей в букете после стягивания всех возможных ребер.

Путь - это последовательность дуг(ориентированных ребер) в ориентированном графе, такая, что конец одной дуги является началом другой дуги.

Вершинной связностью æ графа G называется наименьшее число вершин, удаление которых приводит к несвязному или тривиальному графу.
Реберной связностью λ графа G называется наименьшее количество ребер, удаление которых приводит к несвязному или тривиальному графу.

Дерево — связный граф (т.е.∃ путь между любой парой вершин), не содержащий циклов.

Разрез — множество ребер, при удалении которых граф теряет связность.

Разрез (в случае транспортной сети) - пара множеств вершин A, B :

1)A ∪ B = V, V - множество всех вершин графа.

2)A ∩ B = ∅

3)s ∈ A, t ∈ B , где s-исток, t-сток.

Транспортная сеть — ориентированный граф $G = (V, E)$, в котором каждое ребро $(u, v) \in E$ имеет неотрицательную пропускную способность $c(u, v) \geq 0$ и поток $f(u, v)$. Выделяются две вершины: источник s и сток t такие, что любая другая вершина сети лежит на пути из s в t.

Двудольный граф — это граф $G(V, E)$, такой что множество вершин V разбито на два непересекающихся подмножества V_1 и V_2, причём всякое ребро E инцидентно вершине из V_1 и вершине из V_2 (то есть соединяет вершину из V_1 с вершиной из V_2). Двудольный граф называется «полным», если любые две вершины из V_1 и V_2 являются смежными.
Паросочетание — это множество попарно несмежных рёбер, то есть рёбер, не имеющих общих вершин.
Совершенное паросочетание из A в B — это паросочетание, в котором участвуют все вершины из A. То есть, любая вершина множества A инцидентна ровно одному ребру, входящему в паросочетание.
Наибольшее паросочетание — это такое паросочетание M в графе G, которое не содержится ни в каком другом паросочетании этого графа, то есть к нему невозможно добавить ни одно ребро, которое бы являлось несмежным ко всем ребрам паросочетания.
Максимальное паросочетание — это такое паросочетание, которое содержит максимальное количество рёбер. У графа может быть множество максимальных паросочетаний. При этом любое максимальное паросочетание является наибольшим, но не любое наибольшее будет максимальным.
Планарный граф — граф, который может быть изображен на плоскости без пересечения ребер.

Валентность вершины — количество рёбер графа G, инцидентных(т.е. соединенных с вершиной) вершине *x*.

Остовное дерево — ациклический(т.е. без циклов) связный подграф(т.е. граф, содержащий некое подмножество вершин данного графа и некое подмножество инцидентных им рёбер.) данного связного неориентированного графа, в который входят все его вершины.

Поток - функция $f: \underline{E} \to R$, где E- множество ориентированных ребер графа, такая, что

1)$f(\vec{e}) = -f(\overleftarrow{e}), \forall e \in \underline{E}$

2)$\sum_{e \in E} f(\underline{e}) = 0, \forall v \in V$- правило Кирхгофа.(по народному: сколько в вершину втекло, столько из нее и вытекло)

Мощность потока — это величина, равная сумме потоков из источника (или сумме потоков в сток, одно и тоже).

Градиент функции, заданной на вершинах графа:

Дан граф и на его вершинах стоят числа $v_1, v_2, ..., v_n$ (задана функция). Градиент этой функции - функция, ставящая каждому ребру в соответствие число и направление, причём число равно разнице между v_i и v_j, где v_i - конец ребра, v_j - начало ребра.

Кольцо — это множество M, на котором заданы две бинарные операции: + и × (называемые сложение и умножение), со следующими свойствами, выполняющимися для любых $a, b, c \in M$:

1. $a + b = b + a$ — коммутативность сложения;
2. $a + (b + c) = (a + b) + c$ — ассоциативность сложения;
3. $\exists 0 \in R \ (a + 0 = 0 + a = a)$ — существование нейтрального элемента относительно сложения;
4. $\forall a \in R \, \exists b \in R \, (a + b = b + a = 0)$ — существование противоположного элемента относительно сложения;
5. $(a \times b) \times c = a \times (b \times c)$ — ассоциативность умножения(ассоциативное кольцо)
6. $\begin{cases} a \times (b + c) = a \times b + a \times c \\ (b + c) \times a = b \times a + c \times a \end{cases}$ — дистрибутивность.
7. $\exists e \in R \, \forall a \in R \, (a \times e = e \times a = a)$ (кольцо с единицей)
8. $\forall a, b \in R \, (a \times b = b \times a)$ (коммутативное кольцо)

Поле - кольцо(1-6) +

1) $\forall a \in M, a \neq 0 \, \exists a^{-1} \in M: a^{-1}a = aa^{-1} = 1$

2)$0 \neq 1, |M| > 1$

Изоморфизм колец. Пусть F_1 и F_2 - кольца. Биекция $f : F_1 \to F_2$ называется изоморфизмом, если для любых $a, b \in F_1$ выполняется

1. $f(a) + f(b) = f(a + b)$
2. $f(a) \cdot f(b) = f(a \cdot b)$
3. $f(e_1)=e_2$, $e_1 \in F_1, e_2 \in F_2$

Неприводимый многочлен - многочлен, который нельзя разложить на нетривиальные (неконстантные) многочлены.

Отображение Фробонениуса: $\Phi: F_p \to F_p$, линейное отображение над F_p, $\Phi(x)=x^p$

Алгоритмы

1. Алгоритм нахождения кратчайшего пути в графе (два варианта). **(ТР 3)**

Есть два алгоритма и их различие в том, что берутся разные веса ребер:
а) вес ребра равен 1 ($w(e_i) = 1$).
б) данный вес ребра.

Общий алгоритм нахождения кратчайшего пути в графе: Из начальной точки *S* прошли в каждую соседнюю точку и закрепили за каждой из этих точек число, которое говорит о том, сколько идти из точки *S* в данную. Т.е. на первом этапе мы записываем веса ребер, по которым прошли. А на последующих этапах суммируем вес ребра и значение точки, из которой выходим. Причем, если попадаем в точку, в которой уже есть какое-то значение, то значение в точке и значение суммы сравниваются и в точку записывается наименьшее значение.

2. Жадный алгоритм нахождения остовного дерева максимального веса. **(ТР 5)**

Каждый раз берем ребро максимального веса, причем если это ребро образует цикл, то про него мы забываем и берем следующее ребро максимального веса из оставшихся и так до тех пор, пока у нас не останется ребер, не считая тех, про которые мы забыли (они не будут входить в остов, все остальные будут).

3. Алгоритм Форда-Фалкерсона. **(ТР 7)**

Алгоритм Форда-Фалкерсона заключается в поиске максимального потока из начальной точки *S* в конечную *t*:

1. Выбираем один случайный путь l из *S* в *t* такой, что $c(\vec{e}) > 0 \ \forall \ \vec{e} \in \vec{l}$.

Путь l нашли, $c = min\ c(\vec{e}), \ \vec{e} \in \vec{l}$.

2. Устроим новую транспортную сеть, в которой по одному ребру можно ходить в обе стороны, причем:

UV: $c(\vec{e}) := c(\vec{e}) - x(\vec{e})$

VU: $c(\overleftarrow{e}) := c(\overleftarrow{e}) + x(\vec{e})$

где U и V - вершины ребра, x - число, которое уже было записанно (оно может = 0), c(e) - мощность.

Ищем в этой транспортной сети новый путь такой, что

$c(\vec{e}) > 0 \ \forall \ \vec{e} \in \vec{l}$.

3. Если нашли, то складываем новый путь с предыдущим.
4. (2) и (3) делаем делаем до тех пор, пока не перестанем находить новые пути, что будет означать, что задача выполненна.

4. Венгерский алгоритм. **(ТР 8)**

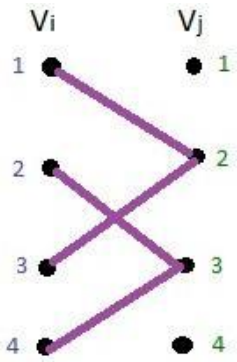
Венгерский алгоритм заключается в ответе на вопрос: “Существует ли совершенное паросочетание в данном графе?” — с семинаров. (От себя: это алгоритм нахождения максимального паросочетания, т.е. паросочетания, которое содержит максимальное число ребер, т.е. паросочетания с большим числом рёбер не существует)

1. Произвольным образом выбираем пары (выделяем их “толстыми”)

2. Необходимо сделать чередующуюся “цепь”, где вправо идем только по тонким ребрам, а влево - только по толстым.
3. Находим любую “цепь”, которая начинается и заканчивается тонким ребром.
Если такой “цепи” нет, то алгоритм закончен. Если такая “цепь” есть, то переходим дальше.
4. “Перекрашиваем” эту “цепь”: теперь те, что в “цепи” были тонкими, делаем толстыми, а те, что были толстыми, делаем тонкими.
5. Переходим к шагу (2).

5. Алгоритм нахождения оптимального назначения. **(ТР 8)**

Есть таблица V состоящая из работников (строки, V_i) и работ (столбцы, V_j). Каждая ячейка C_{ij} говорит о том, с какой эффективностью V_i -ый работник может делать V_j -ую работу.
1. Для каждой строки присваиваем метку α_i , равную максимальному значению в этой строке, т.е. для каждого работника находим работу, которую он делает с максимально возможной для себя эффективностью и ставим метку α_i, равную этой эффективности. Для каждого столбца присваиваем метку $\beta_j = 0$.
2. Теперь пусть каждая строка и каждый столбец таблицы будет обозначать вершину графа и пусть V_i и V_j вершины соединены ребром, когда выполняется условие $\alpha_i + \beta_j = c_{ij}$, так как нам нужна максимальная эффективность (общее условие: $\alpha_i + \beta_j \geq c_{ij}$, которое всегда выполняется)
Строим граф, в который входят все вершины исходного графа и найденные ребра.
3. В построенном графе ищем максимальное паросочетание. Если найденное паросочетание совершенно, то алгоритм закончен. Если нет, то идем дальше.



4. Из теоремы Холла существует подмножество x из V_i и S(x) из V_j : $|x| > |S(x)|$.
Найдём эти подмножества:
V_i - вершины, соответствующие номеру столбца, V_j - вершины, соответствующие номеру строчки.
Во множестве V_i находим такое подмножество x, которое соединено с меньшим подмножеством S(x), которое находится во множестве V_j (т.е. обязательное условие $|x| > |S(x)|$)
На примере рисунка можно выбрать различные такие пары множеств:
1) $V_i \ni x = \{1, 3\}, \Rightarrow V_j \ni S(x) = \{2\}$
2) $V_i \ni x = \{2, 4\}, \Rightarrow V_j \ni S(x) = \{3\}$
3) $V_i \ni x = \{1, 2, 3, 4\}, \Rightarrow V_j \ni S(x) = \{2, 3\}$
- это все возможные варианты выбора x и S(x) для данного графа.
Для каждой вершины V_i из x метку α_i уменьшаем на 1, а для каждой вершины V_j из S(x) метку β_j увеличиваем на 1.
5. Переходим на начало шага 2 с новыми значениями меток.

Вычисления в конечных полях
(ТР 9)

1. проверка неприводимости многочлена над конечным полем

Для того, чтобы показать, что многочлен неприводим, в многочленах 2 и 3 степени достаточно доказать, что корней над данным полем нет. Для этого (как вариант) перебрать все возможные значения и посмотреть чему будет равен многочлен.
Если ни одно из значений не даст нуля ⇒ многочлен неприводим.
Но это работает только для многочлена 2 и 3 степени. Для многочленов большей степени надо смотреть возможность разложения на множители, например: $x^4+2x^2+1=(x^2+1)^2$ (на экзамене такого не должно быть, т.к. чтоб проверить многочлен большей степени, надо затратить очень много времени, обычно это программируют)

2. Перечисление неприводимых многочленов малых степеней над малыми конечными полями

На примере:
n = 4, p = 2;
Ищем многочлен степени 4 над $\mathbf{F}_2$. ($\mathbf{F}_2 = \{0, 1\}$)
Итог: 3 неприводимых многочлена 4 степени над полем $\mathbf{F}_2$:
1) $x^4 + x^3 + x^2 + x + 1$
Смотря на этот многочлен, находим все возможные варианты других многочленов 4 степени, т.е. обязательно многочлен начинается с x^4, и обязательно в многочлене должна присутствовать 1. Т.к. если ее не будет, то многочлен можно будет разложить на множители, например вынести x.
Многочлен x^4+1 не является неприводимым над полем $\mathbf{F}_2$, т.к. его можно представить как $(x^2+1)(x^2+1)$
Многочлен $x^4 + x^2 + 1$ - приводимый, т.к. можно представить как $(x^2+x+1)(x^2+x+1)$
Многочлен $x^4 + x^3 + x^2 + 1$ - приводим, т.к. можно представить как $(x+1)(x^3+x+1)$
Многочлен $x^4 + x^2 + x + 1$ - приводим, т.к. можно представить как $(x+1)(x^3+x^2+1)$
2) Многочлен $x^4 + x^3 + 1$ - неприводимый
3) Многочлен $x^4 + x + 1$ - неприводимый
Неперечисленные возможные многочлены можно аналогично разложить на множители, т.е. они приводимы.

3. Построение конечного поля из p^n элементов

Существует единственное поле из p^n элементов, которое получается из любого неприводимого многочлена $P(x) = x^n + a_1x^{n-1}+...+a_n$

$\mathbf{F}_p$ ($=\mathbb{Z}_p$) = $\{\underline{0}, \underline{1}, \ldots, \underline{p-1}\}$ - поле.

$\mathbf{F}_p[x]/(P(x))$ = {остатки от деления на P(x)} = {многочлены степени < n} = $\{b_0+b_1x+...+b_{n-1}x^{n-1}, b_i \in \mathbf{F}_p\}$ - их кол-во = p^n
Т.к. P(x) - неприводимый многочлен, то $\mathbf{F}_p[x]/(P(x))$ - поле. (Аналогично когда n-простое, то $\mathbb{Z}_n$ - поле)

4.Нахождение порядка заданного элемента (по умножению)

1. Возводить элемент в степень, пока в определенной степени не получится 1. Эта степень будет порядком элемента.

2. Если порядок элемента α равен m, порядок элемента β равен k и (m, k) = 1. То порядок элемента (αβ) равен mk

3. (Рассматриваем многочлены степени n-1 $(b_0+b_1\alpha+...+b_{n-1}\alpha^{n-1})$ из поля $\mathbf{F}_p[x]/(P(x))$; α пишем вместо x лишь для того, чтобы понимать, что эти многочлены являются элементами поля).
Представляем, что многочлен $c_0+c_1\alpha+...+c_{n-1}\alpha^{n-1}$ — многочлен, равный $(b_0+b_1\alpha+...+b_{n-1}\alpha^{n-1})^m$.
Тогда $(b_0+b_1\alpha+...+b_{n-1}\alpha^{n-1})^{m+1} = (c_0+c_1\alpha+...+c_{n-1}\alpha^{n-1})(b_0+b_1\alpha+...+b_{n-1}\alpha^{n-1})$.
Раскрывая скобки, получим новые коэффициенты $c_0,...,c_{n-1}$. Тем самым получим рекуррентную формулу. Стоит отметить, что из многочлена n-ой степени (P(x)), приравнивая его к 0, выражается элемент n-ой степени, чтобы при перемножении $(c_0+c_1\alpha+...+c_{n-1}\alpha^{n-1})(b_0+b_1\alpha+...+b_{n-1}\alpha^{n-1})$ понижать степень и получать опять многочлен степени n-1.

Пример:

$P(x) = x^2+kx+l$ - неприводимый многочлен в $\mathbf{F}_{13} \Rightarrow \alpha^2+k\alpha+l = 0 \Rightarrow \alpha^2 = -k\alpha-l$
Рассмотрим поле $(\mathbf{F}_{13}[x]/(P(x)))^* = (\mathbf{F}_{13}[x]/(x^2+kx+l))^*$ = {многочлены степени = 1} = {1, 2, …, 12, α, 1+α, 2+α, …, 12+α, …, 12α, 1+12α, 2+12α, …, 12+12α}
Возьмем элемент 3+12α, найдем его порядок:
Предположим, что $(3+12\alpha)^m = a+b\alpha$
Тогда $(3+12\alpha)^{m+1} = (3+12\alpha)^m(3+12\alpha) = (a+b\alpha)(3+12\alpha) = 3\alpha+3b\alpha+12a\alpha+12b\alpha^2 = 3a + (3b+12a)\alpha +$
$+12b(-k\alpha-l) = 3a + (3b+12a)\alpha -12bk\alpha - 12bl = (3a - 12bl) + (3b+12a-12bk)\alpha = (3a - 12bl) + ((3-12k)b+12a)\alpha$
Подводя итоги получим:

	c_1	c_2
Для $(3+12\alpha)^m$	a	b
Для $(3+12\alpha)^{m+1}$	3a-12bl	(3-12k)b+12a

С помощью такой рекуррентной формулы быстрее найти порядок элемента 3+12α.
P.S. если взять k=1, l=-1, то многочлен $P(x) = x^2+kx+l = x^2+x-1$ - неприводим в поле $\mathbf{F}_{13}$.

Теоремы

1. Корректность алгоритма нахождения кратчайшего пути в графе.

1. Алгоритм завершится, так как на каждом повторе помечается хотя бы одна вершина, а их конечное количество.
2. Полученный ответ является верным, так как на каждом повторе получается верный ответ.

2. Корректность жадного алгоритма.

Док-во того, что остовное дерево, найденное жадным алгоритмом самое тяжелое.
Пусть Δ - остовное дерево, найденное жадным алгоритмом. Его ребра: $e_1, e_2, ..., e_i$. Причем упорядочные по весу.
Пусть Δ' - другое остовное дерево. Его ребра: $f_1, f_2, ..., f_m$. Причем упорядочные по весу.
Необходимо док-ть, что $\sum_1^i w(e_i) \geq \sum_1^m w(f_m)$.
Пусть $e_1=f_1, e_2=f_2, \ldots, e_k=f_k$, т.е. до k-ого ребра эти деревья совпадают и пусть начиная с k+1 ребра — $f_{k+1} \neq e_{k+1}$.
Учитывая, что в жадном алгоритме всегда берется ребро максимального веса и не образующее циклов $e_{k+1} \geq f_{k+1}$.
Т.к. Δ и Δ' — деревья, $g(\Delta') = 0$, т.к. цикломатическое число любого дерева равно 0.
Добавляя ребро e_{k+1} к Δ' получаем $g(\Delta' \cup \{e_{k+1}\}) = 1$ и e_{k+1} образует цикл $\Rightarrow \Delta' \cup \{e_{k+1}\}$ не дерево.
Вопрос: может ли быть так, что все ребра, образующие этот цикл - это ребра $f_j : j<k+1$?
Ответ: нет. Потому что по условию $e_1=f_1, \ldots, e_k=f_k$, т.е. если $j<k+1$, то начальное остовное дерево Δ - НЕ будет являться деревом, т.к. будет так же образовывать цикл с e_{k+1}
$\Rightarrow$ в этом цикле есть $f_j : j \geq k+1$, т.е. можно сделать вывод, что $w(f_j) \leq w(e_{k+1})$
$\Rightarrow$ получаем новое остовное дерево $\Delta'' = (\Delta' \cup \{e_{k+1}\}) \setminus \{f_j\} \Rightarrow w(\Delta'') \geq w(\Delta')$, причем в Δ'' есть ребра $e_1, \ldots, e_{k+1} \in \Delta$.
Таким образом можно получать новые остовные деревья, в которых с каждым разом будет всё больше ребер из Δ. Так можно делать до тех пор, пока не получится остовное дерево Δ, найденное жадным алгоритмом.

3. Корректность алгоритма Форда-Фалкерсона.

Формулировка: величина максимального потока в транспортной сети равна величине пропускной способности его минимального разреза.
Док-во:

Сумма потоков из s равна потоку через любой разрез, в том числе минимальный $\Rightarrow$ не превышает пропускной способности минимального разреза. Следовательно, максимальный поток не больше пропускной способности минимального разреза. Осталось доказать, что он и не меньше её. Пускай поток максимален. Тогда в остаточной сети сток не достижим из источника, т.е. нет другого пути, по которому можно было бы пройти из S в t. Пусть A - множество вершин, достижимых из источника в остаточной сети, B - недостижимых. Тогда, поскольку $s \in A, t \in B$, то (A,B) является разрезом. Кроме того, в остаточной сети не существует ребра (a,b) с положительной пропускной способностью, такого что $a \in A, b \in B$, иначе бы b было достижимо из s. Следовательно, в исходной сети поток по любому такому ребру равен его пропускной способности, и, значит, поток через разрез (A,B) равен его пропускной способности. Но поток через любой разрез равен суммарному потоку из источника, который в данном случае равен максимальному потоку. Значит, максимальный поток равен пропускной способности разреза (A,B), которая не меньше пропускной способности минимального разреза. Теорема доказана.

4. Корректность венгерского алгоритма.

Алгоритм корректен, так как рёбер конечное число. Алгоритм даёт верный ответ, так как на каждом повторе рёбер в паросочетании становится больше, но при этом их количество ограничено. В итоге получается максимальное паросочетание.

5. Корректность алгоритма нахождения оптимального назначения.

6. Формула для рода графа.

Род графа (цикломатическое число) g=P-B+1
Найдём в графе остовное дерево. Очевидно, что в него входят B-1 рёбер. Род графа - число рёбер, не входящих в остовное дерево = P-(B-1) = P-B+1.

7. Связный граф без циклов имеет род 0 и наоборот. (Равносильность двух определений дерева.)

Связь между числом вершин и ребер дерева.

Род графа (цикломатическое число) g=P-B+1, где P- число ребер графа, B - число вершин.
В дереве P=B-1.
Если g=P-B+1=0 ⇒ P=B-1 ⇒ Данный граф - дерево. И наоборот, если данный граф - дерево, то P=B-1 ⇒ g=P-B+1=B-1-B+1=0

8. Связь между числами реберной и вершинной связности.

Теорема Уитни.
Для любого графа G справедливо неравенство : $\kappa \leq \lambda \leq \delta$
где δ- это минимальная степень вершины графа G, κ-вершинная связность, λ-реберная связность
Док-во:

1. Проверим второе неравенство. Если в графе G нет ребер, то $\lambda = 0$. Если ребра есть, то несвязный граф получаем из данного, удаляя все ребра, инцидентные вершине с наименьшей степенью. В любом случае $\lambda \leq \delta$.
2. Чтобы проверить первое неравенство нужно рассмотреть несколько случаев.
    1. Если G - несвязный или тривиальный граф, то $\kappa = \lambda = 0$.
    2. Если G связен и имеет мост x, то $\lambda = 1$. В последнем случае$\kappa = 1$, поскольку или граф G имеет точку сочленения, инцидентную ребру x, или же $G = K_2$.
    3. Наконец, предположим, что граф G содержит множество из $\lambda \geq 2$ ребер, удаление которых делает его несвязным. Ясно, что удаляя $\lambda - 1$ ребер из этого множества получаем граф, имеющий мост $x = uv$. Для каждого из этих $\lambda - 1$ ребер выберем какую-либо инцидентную с ним вершину отличную от u и v. Удаление выбранных вершин приводит к удалению $\lambda - 1$ (а возможно, и большего числа) ребер. Если получаемый после такого удаления граф не связен, то $\kappa < \lambda$; если же он связен, то в нем есть мост x, и поэтому удаление вершины u или v приводит либо к несвязному, либо к тривиальному графу. В любом случае $\kappa \leq \lambda$.

Замечание.

Для любых натуральных чисел a, b, c, таких что $a \leq b \leq c$, существует граф G, у которого $\kappa = a, \lambda = b$ и $\delta = c$

Док-во:

Рассмотрим граф G, являющийся объединением двух полных графов G_1 и G_2, содержащих $c + 1$ вершину. Отметим bвершин, принадлежащих подграфу G_1 и a вершин, принадлежащих подграфу G_2. Добавим в граф G b ребер так, чтобы каждое ребро было инцидентно помеченной вершине, лежащей в подграфе G_1 и помеченной вершине, лежащей в подграфе G_2, причем не осталось ни одной помеченной вершины, у которой не появилось хотя бы одно новое ребро, инцидентное ей. Тогда:

1. Поскольку $b \leq c$, то было как минимум две непомеченные вершины, поэтому $\delta = c$, так как минимальные степени вершин графов G_1 и G_2 были равны c, а степени их вершин не уменьшались.
2. Заметим, что между двумя вершинами графа G существует не меньше a вершинно-непересекающихся простых цепей, следовательно по теореме Менгера $\kappa \geq a$. Однако если удалить из графа G помеченные вершины его подграфа G_2, то граф G потеряет связность. Значит, $\kappa = a$.
3. Аналогично рассуждению пункта 2, легко убедится, что $\lambda = b$.

9. Критерий эйлеровости графа.

Эйлеровым путем в графе называется путь, который проходит по каждому ребру, причем ровно один раз. Эйлеров цикл — замкнутый эйлеров путь.
Граф называется эйлеровым, если он содержит эйлеров цикл. Граф называется полуэйлеровым, если он содержит эйлеров путь, но не содержит эйлеров цикл.

Критерий эйлеровости:

Для того, чтобы граф $G = (V, E)$ был эйлеровым, нужно, чтобы все вершины имели четную валентность.

Док-во:

Допустим в графе существует вершина с нечетной валентностью. Рассмотрим обход графа. Заметим, что при попадании в вершину и при выходе из нее мы уменьшаем ее валентность на два (помечаем уже пройденые ребра), если эта вершина не является стартовой(она же конечная для цикла). Для стартовой(конечной) вершины мы уменьшаем ее валентность на один в начале обхода эйлерова цикла, и на один при завершении. Следовательно вершин с нечетной валентностью быть не может. Наше предположение неверно.

10. Множество потоков является линейным пространством, размерность которого равна роду графа.

Утв. Множество потоков является линейным пространством.
Док-во: Докажем, что множество потоков является линейным подпространством пространства векторов. Определим операции сложения потоков и умножения на число:

Пусть

f: E → R g: E → R

f(e) → r_1 g(e) → r_2

а)$(f+g)(\underline{e}) = f(\underline{e}) + g(\underline{e}), \underline{e} \in \underline{E}, f, g$-потоки

б)$(c \cdot f)(\underline{e}) = c \cdot (f(\underline{e})),\ \underline{e} \in \underline{E}\ c \in R, f$-поток

Докажем, что операции а, б замкнуты на множестве потоков.

а) Проверим что $f+g$ - поток

1)$(f+g)(e^{\leftarrow}) = f(e^{\leftarrow}) + g(e^{\leftarrow}) = -f(e^{\rightarrow}) + (-g(e^{\rightarrow})) = -(f+g)e^{\rightarrow}$

2) $\sum_{\underline{e_+} \in S(v)} (f+g)(\underline{e}) = \sum_{e_+ \in S(v)} f(\underline{e}) + \sum_{e_+ \in S(v)} g(\underline{e}) = 0+0=0$

1,2 $\Rightarrow$ $f+g$- поток.

б) Проверим, что $C \cdot f$- поток.

3)$(C \cdot f)(e^{\leftarrow}) = C \cdot f(e^{\leftarrow}) = C \cdot (-f(e^{\rightarrow})) = -(C \cdot f)e^{\rightarrow}$

4) $\sum_{\underline{e_+} \in S(v)} (C \cdot f)(\underline{e}) = C \cdot \sum_{e_+ \in S(v)} f(\underline{e}) = C \cdot 0 = 0$

3,4 $\Rightarrow$ $C \cdot f$- поток.

а, б$\Rightarrow$ Множество потоков является линейным подпространством $\Rightarrow$ множество потоков - линейное пространство.

Так как множество потоков - линейное пр-во, то у него есть базис и размерность пространства равна количеству элементов базиса. Найдём остовное дерево. Во множестве потоков есть потоки, в которых проходит 1 по одному из рёбер, не входящих в остовное дерево, и по рёбрам остовного дерева возвращается к начальному ребру. Каждому из таких рёбер соответствует один поток $\Rightarrow$ таких потоков g штук. Они образуют базис пространства потоков, так как линейно независимы (очевидно) и через них можно выразить любой поток:

Пусть есть поток X; X на ребре e_i = $X(e_i)$. ξ - базис (ещё не доказано). Вычтем из X сумму $X(e_i)$*ξ:

$X - \sum_{e_i} X(ei)*\xi$, полуичим граф, где на рёбрах остовного дерева стоят какие-то числа, а на остальных рёбрах нули. Так как для потоков должно выполняться правило Кирхгоффа, то у рёбер, граничащих с неостовными получается тоже 0, дальше по индукции получается, что на всех рёбрах 0 $\Rightarrow$

$X = \sum_{e_i} X(ei)*\xi$, то есть любой поток на графе можно выразить через ξ, т.е. ξ - базис, в нём g элементов $\Rightarrow$ размерность пространства потоков равна роду графа.

11. Множество градиентов является линейным пространством, размерность которого на единицу меньше числа вершин.

12. Базис пространства потоков, связанный с остовным деревом.

См. 10й вопрос.

13. Поток в траспортной сети. Определение мощности потока.

Транспортная сеть - граф, в котором существуют начальная и конечная вершины (S и t соотвественно).

Поток: Пусть $\underline{E}$ - мн-во ориетированных ребер, V - мн-во вершин. Поток, называется ф-ция $x: \underline{E} \rightarrow \mathbb{R}$ такая, что:

а) $x(e^{\rightarrow}) = -x(e^{\leftarrow})$ ($e^{\rightarrow}$ и $e^{\leftarrow}$ - ребро e, направленное в одну сторону и в противоположную)

б) выполняется правило Кирхгофа: $\forall v \in V \ \sum_{\underline{e} \in S_+(v)} x(e) = 0$

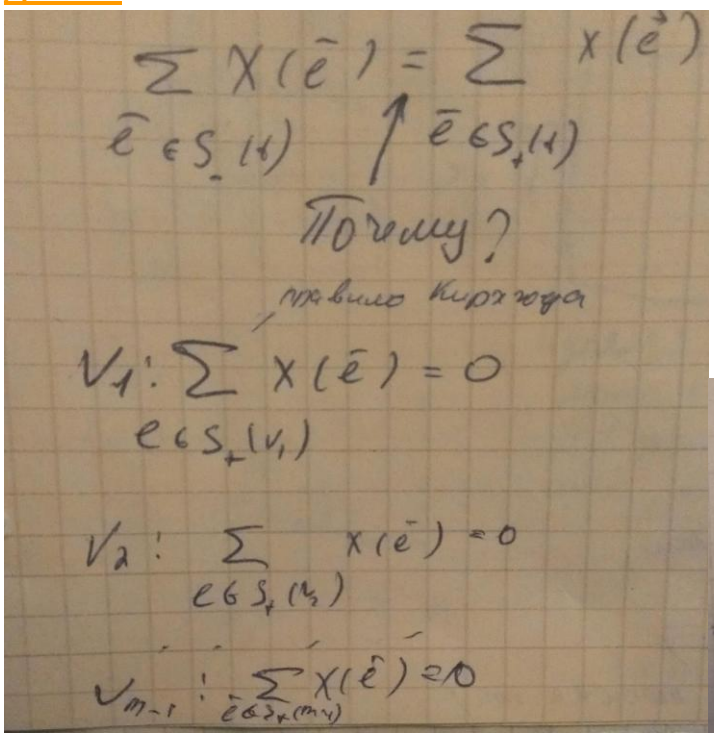
Поток в Транспортной сети - это поток, для которого правило Кирхгофа выполняется всюду, кроме S и t.

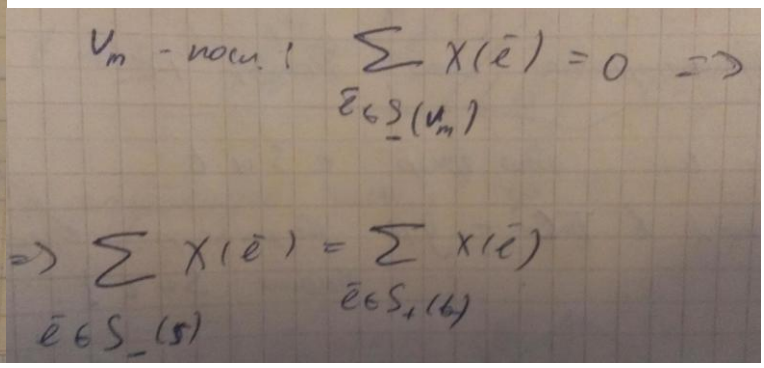
Мощность потока - сумма по всем ребрам вышедшим из S (1) или вошедшим в t (2).

Теорема.

$\sum_{e \in S_-(t)} x(e) = \sum_{e \in S_+(S)} x(e) = C$, т.е. условия (1) и (2) эквивалентны

Док-во.





14. Сумма значений потока в транспортной сети на ребрах любого разреза равна мощности потока.

15. Теорема Форда-Фалкерсона.

Формулировка: величина максимального потока в транспортной сети равна величине пропускной способности его минимального разреза.

Док-во:

Сумма потоков из s равна потоку через любой разрез, в том числе минимальный ⇒ не превышает пропускной способности минимального разреза. Следовательно, максимальный поток не больше пропускной способности минимального разреза. Осталось доказать, что он и не меньше её. Пускай поток максимален. Тогда в остаточной сети сток не достижим из источника, т.е. нет другого пути, по которому можно было бы пройти из S в t. Пусть A - множество вершин, достижимых из источника в остаточной сети, B - недостижимых. Тогда, поскольку $s \in A, t \in B$, то (A,B) является разрезом. Кроме того, в остаточной сети не существует ребра (a,b) с положительной пропускной способностью, такого что $a \in A, b \in B$, иначе бы b было достижимо из s. Следовательно, в исходной сети поток по любому такому ребру равен его пропускной способности, и, значит, поток через разрез (A,B) равен его пропускной способности. Но поток через любой разрез равен суммарному потоку из источника, который в данном случае равен максимальному потоку. Значит, максимальный поток равен пропускной способности разреза (A,B), которая не меньше пропускной способности минимального разреза. Теорема доказана.

16. Теорема Менгера (реберная).

Теор. Между вершинами u и v существует L реберно непересекающихся путей тогда и только тогда, когда после удаления любых $(L-1)$ ребер существует один путь из u в v.

Для доказательства используются следующие утверждения:

Утв1 Если пропускные способности всех ребер целочисленные (сеть целочислена), то существует максимальный поток, целочисленный на каждом ребре.

Док-во:

Для доказательства достаточно рассмотреть алгоритм Форда-Фалкерсона для поиска максимального потока. Алгоритм делает примерно следующее (подробней - читай в соответствующей статье):
1. В начале берем какой-нибудь поток за начальный (например, нулевой).
2. В остаточной сети этого потока находим какой-нибудь путь из источника к стоку и увеличиваем поток на пропускную способность этого пути.
3. Повторяем пункт 2 до тех пор, пока находится хоть какой-то путь в остаточной сети.
То, что получится в конце, будет максимальным потоком. В случае целочисленной сети достаточно в качестве начального приближения взять нулевой поток, и не трудно видеть, что на каждой итерации (в том числе и последней) этот поток будет оставаться целочисленным, что и докажет требуемое.

Утв2: Если в сети, где все пропускные способности ребер равны 1, существует целочисленный поток величиной L то существует и L реберно непересекающихся путей.

Док-во: Считаем, что u - источник, v - сток.

В начале поймем, что если поток не нулевой, то существует маршрут из u в v лежащий только на ребрах с потоком равным 1. В самом деле, если бы такого маршрута не существовало, то можно было бы выделить множество вершин до которых такие маршруты из вершины u существуют, не включающее v, и по нему построить разрез. Поток через такой разрез, очевидно равен нулю, видим противоречие (т.к. $f(U,V) = |f|$, смотри утв. 1).
Итак, найдем какой-нибудь маршрут из u в v лежащий только на ребрах где поток равен 1. Удалив все ребра находящиеся в этом маршруте и оставив все остальное неизменным, придем к целочисленному потоку величиной $L-1$. Ясно, что можно повторить тоже самое еще $L-1$ раз, и, таким образом мы выделим L реберно непересекающихся маршрутов.

Док-во:

$\Leftarrow$
Пусть u - источник, а v - сток.
Назначим каждому ребру пропускную способность 1. Тогда существует максимальный поток, целочисленный на каждом ребре (Утв1).
По теореме Форда-Фалкерсона для такого потока существует разрез с пропускной способностью равной потоку. Удалим в этом разрезе $L-1$ ребер, и тогда, раз u и v находятся в разных частях разреза и, существует путь из u в v, то в разрезе останется хотя бы еще одно ребро. Это значит, что пропускная способность разреза и вместе с ним величина потока не меньше L. А так как поток целочисленный, то это и означает, что $\exists L$ реберно непересекающихся путей.

$\Rightarrow$
$\exists L$ реберно непересекающихся путей, а значит, удалив любые $L-1$ ребер хотя бы один путь останется не тронутым (принцип Дирихле). Это и означает, что существует путь из u в v.

17. Теорема Холла.

Пусть $G(V,E)$ - двудольный граф. L - множество вершин первой доли. R - множество вершин правой доли.

Пусть $X \subset V$. Множество соседей X определим формулой: $N(X) = \{y \in V : (x, y) \in E\}$
Совершенное паросочетание - это паросочетание, в котором участвуют все вершины графа. То есть, любая вершина графа сопряжена ровно одному ребру, входящему в паросочетание.
Теорема Хола:Совершенное паросочетание существует тогда и только тогда, когда для любого $A \subset L$ выполнено $|A| \leq |N(A)|$.
Док-во:

Очевидно, что если существует совершенное паросочетание, то для любого $A \subset L$ выполнено $|A| \leq |N(A)|$. У любого подмножества вершин есть по крайней мере столько же "соседей" ("соседи по парасочетанию").

$\Leftarrow$ В обратную сторону докажем по индукции (будем добавлять в изначально пустое паросочетание P по одному ребру и доказывать, что мы можем это сделать, если P не совершенное). Таким образом, в конце получим что P — совершенное паросочетание.

1. База: Вершина из L соединена хотя бы с одной вершиной из R. Следовательно база верна.
2. Переход: Пусть после $k < n$ шагов построено паросочетание P. Докажем, что в P можно добавить вершину x из L, не насыщенную паросочетанием P. Рассмотрим множество вершин H — все вершины, достижимые из x, если можно ходить из R в L только по ребрам из P, а из L в R по любым ребрам из G. Тогда в H найдется вершина y из R, не насыщенная паросочетанием P, иначе, если рассмотреть вершины H_L (вершины из H принадлежащие L), то для них не будет выполнено условие: $|H_L| > |N(H_L)|$. Тогда существует путь из x в y, который будет удлиняющим для паросочетания P (т.к из R в L мы проходили по ребрам паросочетания P). Увеличив паросочетание P вдоль этого пути, получаем искомое паросочетание. Следовательно предположение индукции верно.

18. Критерий двудольности графа (теорема Кенига).

Формулировка:Граф является двудольным тогда и только тогда, когда его циклы имеют четную длину.
Док-во:

Необходимость. Пусть двудольный граф содержит цикл длины *k*.
Докажем, что *k* – четное число. Концы всех его ребер принадлежат разным долям, поэтому, проходя по циклу, мы каждый раз попадаем из одной доли в другую. На последнем шаге мы возвращаемся в исходную вершину, а значит, делаем четное число таких «переходов», поэтому *k* – четное число.

Достаточность. Пусть граф *G* не содержит циклов нечетной длины, то есть все имеющиеся в нем циклы четной длины. Разделим все вершины графа *G* на две части. В первую часть попадут все вершины, расстояние до которых от фиксированной вершины *v* четное число, и сама вершина *v*, а во вторую – все остальные вершины. Осталось показать, что никакие две вершины, попавшие в один класс не смежны. Предположим противное, то есть некоторые вершины *x* и *y*, принадлежащие одному из двух полученных множеств, смежны. Рассмотрим цикл, полученный в результате объединения ребра (*x; y*) и кратчайших цепей, соединяющих вершины *x* и *y* с вершиной*v*. Длина этого цикла равна сумме длин этих двух цепей плюс один. Но длины этих двух цепей одинаковой четности, поэтому их сумма – четное число, значит длина получившегося цикла – нечетное число. Пришли к противоречию, значит никакие две вершины, попавшие с один класс, не смежны.

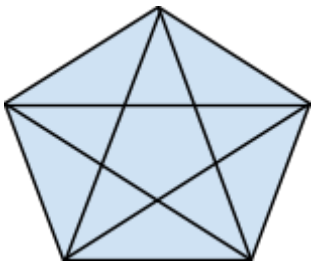
19. Теорема Эйлера о планарных графах.

Формулировка:Для связного плоского графа G верно равенство V − E + F = 2, где V - количество вершин графа G, E- количество ребер графа G, F - количество граней графа G(т.е. число частей, на которые граф делит плоскость).

Доказательство. Пусть на плоскости изображен некоторый граф G. Удалим некоторые ребра из данного графа так, чтобы получилось какое-нибудь остовное дерево этого графа. Поскольку число вершин любого дерева на одну больше числа числа ребер, то для этого дерева E = V − 1, F = 1, и доказываемая формула верна. Теперь начнем восстанавливать исходный граф G из его остовного дерева, для чего будем последовательно добавлять по одному удаленные ребра. При добавлении ребра число вершин никак не меняется, а вот число ребер и число граней увеличивается на 1. Поэтому равенство при добавлении ребра остается верным, а значит окажется верным и после добавления любого числа ребер, в частности для исходного графа G.

20. Непанарность V_5.

Графом V5 называется граф с пятью вершинами, в котором каждая пара вершин соединена ребром.



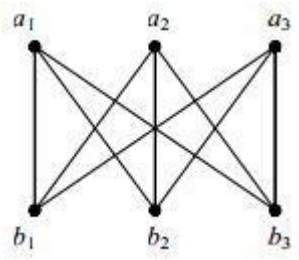
Утв. Граф V5 не планарен.

Док-во:

Допустим, что для графа V5 существует планарная реализация. Так как граф V5 связен, то для этой планарной реализации справедлива формула Эйлера p – q + r = 2. Поскольку в графе V5 имеем p = 5 и q = 10, то число всех граней должно равняться r = 2 – p + + q = 7. Пусть грани занумерованы 1, 2, …, r и пусть при обходе i-ой грани по периметру (по её краю) проходится q_i рёбер. Так как при этом каждое ребро обходится дважды (оно является стороной для двух граней), то $\sum_{i=1}^{r} q_i=2q=20$. Но в каждой грани не менее трёх сторон. Поэтому $q_i \geq 3$ для всех i. Отсюда $\sum_{i=1}^{r} q_i \leq 3r = 21$. Получаем 20 ≥ 21 — противоречие. Значит, для графа V5 не существует планарной реализации.

21. Непланарность $V_{3,3}$.

Графом $V_{3,3}$ называется граф с шестью вершинами a1, a2, a3, b1, b2, b3, в котором каждая вершина a_i соединена ребром с каждой вершиной b_j и других рёбер нет.



Утв: Граф $V_{3,3}$ не планарен.

Док-во:

Допустим, что для графа $V_{3,3}$ существует планарная реализация. Так как граф $V_{3,3}$ связен, то для этой планарной реализации справедлива формула Эйлера p – q + + r = 2. Поскольку в графе $V_{3,3}$ имеем p = 6 и q = 9, то число всех граней должно равняться r = 2 – p + q = 5. Так же, как в доказательстве предыдущей теоремы, получаем, что $\sum_{i=1}^{r} q_i = 2q = 18$, где q_i — число сторон в i-ой грани. Но в графе $V_{3,3}$ нет циклов длины 3. Поэтому в каждой грани не менее 4 сторон. Следовательно, $q_i \geq 4$ для всех i. Отсюда $\sum_{i=1}^{r} q_i \geq 4r = 20$. Получаем $18 \geq 20$ — противоречие. Значит, для графа $V_{3,3}$ не существует планарной реализации.

22. Теорема Понтрягина-Куратовского (б/д).

Теор. Граф планарен ⇔ он не содержит подграфов, гомеоморфных V_5 или $V_{3,3}$

23. Опеределение характеристики поля. Любое конечное поле содержит простое подполе $\mathbf{F}_p$.

Характеристика поля - целое положительное простое число или число 0, однозначно определяемое для данного поля следующим образом: если для $n>0$

$$0 = ne = \underbrace{e + \ldots + e}_{n \text{ слагаемых}},$$

где *e* - единица поля К, то наименьшее из таких *n* будет простым числом и оно называется характеристикой поля *К.* Если же такого числа не существует, то говорят, что характеристика поля К равна нулю, или что *К* - поле нулевой характеристики. Иногда такое поле называется полем без характеристики или полем бесконечной характеристики. Всякое поле нулевой характеристики содержит подполе, изоморфное полю всех рациональных чисел, а поле конечной характеристики *p* - подполе $\mathbf{F}_p$, изоморфное полю классов вычетов по модулю *p.*

24. Теорема о делении многочленов с остатком. Теорема Безу.

Опр. Пусть f и g — многочлены, $g \neq 0$. Будем говорить, что f поделен на g с остатком, если f представлен в виде $f = gq + r$, гдеq и r — многочлены, причем $\deg r < \deg g$.

Полином r называется остатком от деления f на g, q — неполным частным.

Теорема. (о делении с остатком). Пусть f и g — многочлены над полем $\mathbb{K}$, $g \neq 0$. Тогда существуют единственные многочлены q и r над полем $\mathbb{K}$ такие, что $f = qg + r$ и $\deg r < \deg g$.

Доказательство.

∃.

Пусть $\deg f < \deg g$. Положим $q = 0, r = f$.

$\deg f \geq \deg g$.

Предположим, что теорема верна не для любого многочлена f (g фиксируем). Среди всех многочленов f, для которых теорема неверна, выберем многочлен наименьшей степени и обозначим его f_0:
$\deg f_0 = m, \deg g = n, m \geq n.$
Пусть $f_0 = a_0 x^m + \ldots; g = b_0 x^n + \ldots; \qquad (a_0, b_0 \neq 0)$. Положим
$f_1 = f_0 - \frac{a_0}{b_0} x^{m-n} g.$
Коэффициент при x^m в многочлене f_1 равен $a_0 - \frac{a_0}{b_0} \cdot b_0 = 0$. Следовательно, $\deg f_1 < m$. Значит, для многочлена f_1 теорема верна. Существуют такие q_1 и r, что $f_1 = q_1 g + r, \deg r < \deg g$. Тогда
$$f_0 = f_1 + \frac{a_0}{b_0} x^{m-n} g = gq_1 + r + \frac{a_0}{b_0} x^{m-n} g =$$
$$= g \left(\underbrace{q_1 + \frac{a_0}{b_0} x^{m-n}}_{q} \right) + r = gq + r, \deg r < \deg g.$$
Получили противоречие с тем предположением, что есть многочлены, для которых теорема неверна.

!.

Предположим, что
$f = gq + r, \quad \deg r < \deg g,$
$f = gq_1 + r_1, \quad \deg r_1 < \deg g,$
$gq + r = gq_1 + r_1,$
$g(q - q_1) = r_1 - r.$
1) $q = q_1$. Значит, $r = r_1$,
2) $q \neq q_1$.
$\deg (g(q - q_1)) = \deg g + \deg (q - q_1) \geq \deg g,$
$\deg (r - r_1) \leq \max\{\deg r_1, \deg r\} < \deg g.$
Получили противоречие. Этот случай невозможен.

Теорема Безу:остаток от деления многочлена $P(x)$ на многочлен $(x - a)$ равен $P(a)$

Док-во: Поделим с остатком многочлен $P(x)$ на многочлен $x - a$:

$$P(x) = (x - a)Q(x) + R(x).$$

Так как $\deg R(x) < \deg(x - a) = 1$, то $R(x)$ — многочлен степени не выше 0. Подставляя $x = a$, поскольку $(a - a)Q(a) = 0$, имеем $P(a) = R(a)$

25. Многочлен над полем степени *n* имеет не более *n* корней. Пример многочлена над кольцом, имеющего больше корней, чем его степень.

Пример многочлена над кольцом, имеющего больше корней, чем его степень:

$x^2 - 1 = 0$ в $\mathbb{Z}_8$ корни этого уравнения: {1, 3, 5, 7} = {±1, ±3}

26. Теорема о разрешимости диофантова уравнения в кольце многочленов над полем: если

многочлена $A(t)$ и $B(t)$ не имеют общих множителей, то существуют такие многочлены $X(t)$ и $Y(t)$, что $A(t)X(t) + B(t)Y(t) = 1$.

27. Теорема об однозначности разложения многочлена над полем на неприводимые множители. Пример многочлена над кольцом, для которого это не так.

Пример многочлена над кольцом, для которого это не так:

$x^2 - 1=0$ в $\mathbb{Z}_8$ корни этого уравнения: $\{1, 3, 5, 7\} = \{\pm1, \pm3\} \Rightarrow$ этот многочлен можно представить как $(x-1)(x+1) = (x-3)(x+3)$

28. Пусть **K** поле, дан многочлен ненулевой степени $P(t)\in$ **K**[t]. Конструкция фактор-кольца **L** = **K**[t]/$(P(t))$. Доказательство того, что **L** поле тогда и только тогда, когда многочлен $P(t)$ неприводим.

>>> От противного: Если P - приводимый многочлен, то P можно разложить в произведение многочленов P=QR. И Q и R имеют меньшую степень в **L**, т.е. имеют меньший порядок и QR=0, т.е. будут делители нуля $\Rightarrow$ либо Q=0, либо R=0 (по свойству поля) такого быть не может, т.к. Q и R ненулевые многочлены.

<<< Пусть $Q\in$ **L**, $Q = b_0+b_1x+...+b_{n-1}x^{n-1}$, т.е. $\Rightarrow$ P и Q не имеют общих множителей (грубо говоря $(P,Q)=1) \Rightarrow$ Существуют многочлены U(x) и V(x): $P(x)U(x) + Q(x)V(x) = 1$

$QV = P(-U) + 1$, P в **L** $\equiv 0 \Rightarrow QV = 1$

$\Rightarrow$ V - обратный элемент для Q, т.е. для всех элементов из **L** есть обратный элемент $\Rightarrow$ **L** - поле.

29. Пусть **K** поле, дан неприводимый многочлен ненулевой степени $P(t)\in$ **K**[t]. Конструкция фактор-кольца **L** = **K**[t]/$(P(t))$. Доказательство того, что **L** поле тогда и только тогда, когда многочлен $P(t)$ имеет корень в **L**.

30. Конечное поле характеристики p содержит p^n элементов.

$\mathbf{L}=\mathbf{K}[x]/_{P(x)}$, P(x)-неприводим $\Rightarrow$ **L** - поле, причем конечное

Теорема. В любом конечном поле есть подполе $\mathbf{F}_p$, $\mathbf{L}\supset\mathbf{F}_p$

Док-во. в **L** есть операции сложения и умножения на элемент из $\mathbf{F}_p \Rightarrow$ **L** - это линейное пространство над $\mathbf{F}_p$.

Так как **L** - линейное пространство, то существует конечный базис $e_1,e_2,...,e_n$: $\forall\ v \in \mathbf{L} \Rightarrow v=x_1e_1+...+x_ne_n$, $x_i \in \mathbf{F}_p \Rightarrow |\mathbf{L}|=p^n$

31. Любой ненулевой элемент конечного поля из p^n элементов удовлетворяет уравнению $x^{p^n-1}-1 = 0$.

$P(x) = a_0+a_1x+...a_nx^n$ - неприводимый многочлен n-ой степени.

В поле $\mathbf{L}=\mathbf{K}[x]/_{P(x)} = \{b_0+b_1\alpha+...+b_{n-1}\alpha^{n-1}, b_i\in\mathbf{F}_p\}$ p^n элементов, а в поле **L*** — p^n-1, т.к. там присутствуют все элементы, что и в **L**, кроме нулевого $\Rightarrow \forall\ x\in$ **L*** ord x | $(p^n-1) \Leftrightarrow x^{p^{n-1}} = 1, \text{т.е.} x^{p^{n-1}}-1 = 0$

32. Отображение Фробениуса $\Phi(x) = x^p$. Его свойства.

Отображение Форбонениуса: Φ: $x \to x^p$, линейное отображение над F_p, $\Phi(x)=x^p$

Свойства:
$\Phi(ab) = \Phi(a)\Phi(b)$
$\Phi(a+b) = \Phi(a) + \Phi(b)$
$\Phi(\lambda a) = \lambda\Phi(a),\ \ \lambda \in \mathbf{F}_p$

33. Пусть неприводимый многочлен $P(t) \in \mathbf{F}_p[\,t\,]$ степени n имеет в поле $\mathbf{F}_{p^n}$ корень α. Тогда $P(t)$ имеет в $\mathbf{F}_{p^n}$ ровно n различных корней.

34. Конечная подгруппа мультипликативной группы поля циклическая.

35. Многочлен 2 и 3 степени неприводим, если он не имеет корней. Пример приводимого многочлена более высокой степени, не имеющего корней.

Теорема: Многочлен 2 и 3 степени неприводим, если он не имеет корней.
Док-во: Если многочлен степени n приводим, то его можно нетривиальным образом разложить в произведение других многочленов, степень которых k: $1 \le k < n$. В случае, когда n=2 или n=3, получится, что при разложении хотя бы один (а в случае n=2 оба) множитель будут иметь первую степень, т.е. являться многочленами вида (a+bx), что в свою очередь означает, что у исходного многочлена будет как минимум один корень: $x=-b/a \Rightarrow$ неприводимым многочлен 2й или 3й степени будет $\Leftrightarrow$когда у него нет корней!
Пример:
1) $f(x)=x^4+2x^3+3x^2+2x+1=(x^2+x+1)^2=(x^2+x+1)(x^2+x+1)$ - этот многочлен раскладывается нетривиальным образом в произведение многочленов, степень которых ниже степени самого многочлена и не равно 0, однако корней в действительных числах у этого многочлена нет.
2) $f(x)=x^4+2x^2+1 = (x^2+1)^2$ - аналогично корней нет в действительных числах, но раскладывается в произведение двух других многочленов.