«Экология и здоровье человека», Маврикий, 17-24 февраля 2014 г.

Медицинские науки

ОРГАНОМЕТРИЧЕСКИЕ ХАРАКТЕРИСТИКИ ПОДНИЖНЕЧЕЛЮСТНЫХ СЛЮННЫХ ЖЕЛЕЗ ЧЕЛОВЕКА В ПЛОДНОМ ПЕРИОДЕ ОНТОГЕНЕЗА В АРХАНГЕЛЬСКОЙ ОБЛАСТИ

Оправин А.С., Ульяновская С.А., Афоничева Е.Н., Афоничев В.А., Ларионова С.О., Ловцев А.С., Евдокимова Е.Н., Резников М.А.

ГБОУ ВПО «Северный государственный медицинский университет», Архангельск, e-mail: usarambler78@rambler.ru

Слюнные железы играют важнейшую роль в обеспечении нормального состояния полости рта человека. Изучение морфологии поднижнечелюстных слюнных желез актуально и представляет практическую ценность. Выявление закономерностей развития больших слюнных желез может быть полезно как для фундаментальных наук, так и для клинической медицины для разработки мероприятий по предупреждению и лечению целого ряда заболеваний органов пищеварительной системы. Цель работы изучение органометрических характеристик поднижнечелюстных желез плодов человека в Архангельской области.

Исследование выполнено на аутопсийном материале (поднижнечелюстные железы 38 плодов от 10 до 40 недель развития) за период 2012-2013 гг., умерших в родильных отделениях (домах) г. Архангельска, родильном отделении городской больницы № 1 г. Северодвинска. Аутопсийный материал забирался в течение суток после смерти и фиксировался в 10% растворе нейтрального формалина. Затем выполнялось макро- и микроскопическое препарирование с выделением поднижнечелюстных слюнных желез. После чего проводились морфометрические исследования, в ходе которых измерялись масса железы (мг), объем (см3), длина, ширина, толщина (мм). Изучались варианты формы железы по ее контуру (полигональная, овальная, круглая, треугольная). На всех этапах проводилась съемка фотоаппаратом Canon D 500. Секционный материал был разделен на группы в зависимости от возраста и от принадлежности к стороне (правая / левая). Данные статистически обработаны с помощью программы SPSS версия 19,0. Критический уровень статистической значимости принимался за 0,05 (р). Работа одобрена комитетом по этике СГМУ протокол № 02/3-13 от 20.03.13.

Органометрические характеристики поднижнечелюстных желез плодов: масса 76,48 ± 43,025 мг; длина 7,28 ± 1,645 мм; ширина 4,62 ± 0,956 мм; толщина 3,06 ± 0,739 мм; объем 0,13 ± 0,093 $см^3$.

Вариантная анатомия поднижнечелюстных желез: полигональная форма встречалась в 32,43% случаев, овальная и округлая по 24,32%, треугольная – 18,93%. Наиболее часто встречалась полигональная форма поднижнечелюстной железы, что более характерно именно для плодного периода развития человека. В связи с небольшим количеством морфологического материала, не выявлено межгрупповых различий органометрических параметров поднижнечелюстных слюнных желез плодов в возрастных группах ($p>0,05$).

При сравнении желез в зависимости от принадлежности к стороне определено, что среди левых поднижнечелюстных желез преобладала овальная форма (41,17%), среди правых – полигональная форма (51,44%). Органометрия поднижнечелюстных слюнных желез правой и левой сторон показала, что по всем показателям левая подчелюстная слюнная железа имеет большие размеры, чем правая. Наиболее отчетливо выражена разница в средней массе железы – 84,85 ± 55,071 мг (слева), 78,84 ± 35,592 мг (справа).

Результаты проведенного исследования предопределяют дальнейшее изучение процесса развития поднижнечелюстных желез в плодном периоде онтогенеза и выявление факторов, которые оказывают наибольшее влияние на морфологию органа.

«Инновационные технологии», Таиланд, 19-27 февраля 2014 г.

Физико-математические науки

НОВАЯ ТЕОРЕМА О КРИТЕРИИ ПРОСТОГО ЧИСЛА

Акылбаев М.И., Уштенов Е.Р.

Южно-Казахстанский инженерно-педогогический университет дружбы народов, Шымкент, e-mail: musabek_kz@mail.ru

Простые числа приобретают особую важность в теории чисел в силу «фундаментальной теоремы арифметики», гласящей, что каждое составное число может быть представимо одним и только одним способом в виде произведения простых множителей [3, 7].

Первая теорема, утверждающая существование бесконечного множества простых чисел, была доказана уже Евклидом в «Началах», в книге 9, предложение 20 [3, 7].

Под критерием простых чисел понимается теоретико-числовое свойство, которое присуще лишь простым числам и наличие которого может быть установлено независимо от предварительной проверки простого числа. Простым примером является соотношение:

$$\sum_{m=1}^{m=n}\left\{\left[\frac{n}{m}\right]-\left[\frac{n-1}{m}\right]\right\}=2, \qquad (1.1)$$

которое справедливо тогда и только тогда, когда n является простым числом. Так как слагаемые равны 1, если m делитель n, и равны нулю, если это не так, то сумма (конечная) представляет собой число $d(n)$ делителей n, а равенство $d(n)=2$ характеризует простые числа. Естественно, формула (1), как и многие другие критерии, не пригодна для практических целей [6, 30].

Критерием числа на простоту является достаточное условие простоты числа. Кроме достаточных условий простоты числа также существуют необходимые условия.

Необходимым условием простоты числа является теоретико-числовое свойство числа присущее в большей степени простым числам, но это свойство могут иметь некоторые составные числа. Приведем примеры основных необходимых условий простоты числа:

1. Всякое простое число, большее 3, представимо в виде:

$$6k+1 \text{ или } 6k-1. \qquad (1.2)$$

2. Если p – число простое, то верно сравнение:

$$p^2-1\equiv 0 \ (\mathrm{mod}\ 24) \qquad (1.3)$$

3. Если p – число простое, то верны сравнения:

$$a^p\equiv a\ (mod\ p),\ (a,p)=1, \qquad (1.4)$$

и

$$a^{p-1}\equiv 1\ (mod\ p),\ (a,p)=1, \qquad (1.5)$$

что означает, остаток от деления a^{p-1} на p равен 1, и соответственно остаток от деления a^p на p равен a. (Малая теорема Ферма).

Существуют и другие необходимые условия простоты числа. Достаточным условием простоты числа является теоретико-числовое свойство числа присущее простым и только простым числам. Также приведем основные примеры этих условий, основанных на следующих теоремах:

1. Теорема Вильсона. Если p – число простое, то верно сравнение:

$$(p-1)!+1 \equiv 0 \ (\mathrm{mod}\ p) \qquad (1.6)$$

Верно и обратное утверждение.

2. Теорема Лейбница. Если p – число простое, то верно сравнение:

$$(p-2)! - 1 \equiv 0 \ (\mathrm{mod}\ p) \qquad (1.7)$$

Верно и обратное утверждение.

3. Теорема Серпинского. Если число вида $p= 4k+1$ и выполняется условие сравнения:

$$\left(\frac{p-1}{2}\right)!^2 +1 \equiv 0 \ (\mathrm{mod}\ p), \qquad (1.8)$$

то число p – простое [5, 51-53].

Есть и другие теоремы, дающие условия простоты.

Проверка чисел на простоту на сегодняшний день является одним из самых актуальных задач в теории чисел, так как она связана с такой задачей как факторизация числа. Если проверка на простоту числа даст положительный ответ, то есть проверяемое число окажется простым, то операция факторизации числа отпадает. В случае отрицательного ответа встает задача нахождения нетривиальных делителей испытуемого числа.

Существует много тестов на простоту числа: тест Соловея-Штрассена, тест Миллера-Рабина, алгоритм Адлемана, Померанса, Румеля, алгоритм Ленстры, проверка числа теоремой Ферма, алгоритм Ленстры-Коена, алгоритмАдлемана- Хуанга (1972 г.), алгоритм Агравала, Кайалы, Саксены (2002 г.) и другие. Все вышеперечисленные методы и алгоритмы являются полиномиальными и потому являются вероятностными.

На сегодняшний день в криптографии в системе RSA открытым текстом используют многоразрядные числа, которые невозможно проверить на простоту числа со 100 процентной гарантией и невозможно разложить на простые множители (факторизация). Это связано с тем, что проверка больших чисел на простоту требует очень большое число операций, что не под силу даже суперсовременным компьютерам.

В этой статье мы хотим привести недостаток одного детерминированного алгоритма проверки числа на простоту, считающегося наиболее совершенным и потому имеющим широкое практическое применение в криптографии, а также представить новую теорему о критерии простого числа.

В книге Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. Москва, МЦНМО. 2003 г. В главе 1, §1.9 приведен детерминированный алгоритм проверки простоты на туральных чисел индийских математиков Агравала, Кайалы и Саксены (2002 г.),. Он имеет сложность $O(\log^6 n \cdot \ln\ln n)$ арифметических операций (n – проверяемое число, c – некоторая абсолютная константа). Алгоритм основан на следующей теореме.

Теорема 1.71. Пусть p – нечетное натуральное число, $a\in Z(a,p)=1$.

Число p является простым тогда и только тогда, когда

$$(x-a)p \equiv xp - a \ (\mathrm{mod}\ p),\ [4, 48] \qquad (2.1)$$

Мы решили проанализировать эффективность этой теоремы.

Преобразуем левую часть сравнения (2.1) в следующий вид:

$$(x-a)^p = x^p + \sum_{i=1}^{p-1} \binom{\boldsymbol{p}}{\boldsymbol{i}} \boldsymbol{x}^{i+1} (-\boldsymbol{a})^{p-i} - a^p. \quad (2.2)$$

Если p – простое число, то верно сравнение:

$$\sum_{i=1}^{p-1} \binom{\boldsymbol{p}}{\boldsymbol{i}} \boldsymbol{x}^{i+1} (-\boldsymbol{a})^{p-i} = 0 \pmod p, \quad (2.3)$$

и сравнение (2.1) принимает вид:

$$\boldsymbol{x}^p - \boldsymbol{a}^p \equiv \boldsymbol{x}^p - a \pmod p, \quad (2.4)$$

и последнее сравнение равнозначно малой теореме Ферма:

$$\boldsymbol{a}^{p-1} \equiv 1 \pmod p. \quad (2.5)$$

Теперь рассмотрим другой случай, когда p – составное число и притом является числом Кармайкла (псевдопростое числа), например, p_1= 651=3·11·17, p_2 = 2821=7·13·31, p_3 = 10585=5·29·73, p_4 = 15841=7·31·73 и так далее. Чисел Кармайкла бесконечно много [2, 703-722].

Экпериментальные вычисления показывают, что все эти числа пройдут тест на простоту по алгоритму индийских математиков и по малой теореме Ферма и дадут ложный ответ. Далее. При p – являющимся числом Кармайкла, естественно не найдутся числа q и k такие, удовлетворяющие условиям теоремы 1.71.

В связи с этой темой приводим новую теорему в теории чисел по критерию простого числа, являющейся банальным случаем, но не встречающейся в технической литературе.

Теорема о критерии простого числа. Автор – Ущтенов Есенбек Рискулович, авторское свидетельство № 128 от 14.02.2013 год, зарегистрированное в Комитете по правам интелектуальной собственности Министерства юстиции Республики Казахстан.

Теорема. Пусть n – натуральное нечетное число. Если выполняется условие (2.6), то верно утверждение, что n – простое число.

$$\left[\frac{\boldsymbol{n}}{3}\right]! \not\equiv 0 \pmod n \quad (2.6)$$

Искючения составляют только числа n=9 и n=25.

Доказательство.

Так как любое натуральное нечетное составное число может иметь наименьший делитель число 3, то наибольший делитель может быть равным числу $\frac{n}{3}$. В случае, если это число имеет другие делители, то его делители будут находится в зоне между числами 3 и $\frac{n}{3}$.

Как известно, простое число n имеет два тривиальных делителя: 1 и самого себя n, и потому, не имея ни одного делителя от числа 3 и до числа $\frac{n}{3}$, при делении этого простого числа на другие натуральные числа меньшие $\frac{n}{3}$, будут давать остатки от 1 до n–1.

На основании вышесказанного имеет место выражение (2.6).

Рассмотрим исключительные случаи.

Пример 1. Пусть n=9, тогда

$$\left[\frac{\mathrm{n}}{3}\right]! \equiv 6 \left[\frac{9}{3}\right]! = 3!.\ 1\cdot2\cdot3 = 6,$$

и

$$\left[\frac{9}{3}\right]! \equiv 6 \pmod 9, \quad (2.7)$$

Пример 2.

Пусть n=25, тогда

$$\left[\frac{\mathrm{n}}{3}\right]! = \left[\frac{25}{3}\right]! = 8!\ 1\cdot2\cdot3\cdot4\cdot5\cdot6\cdot7\cdot8 = 40320,$$

и

$$\left[\frac{25}{3}\right]! \equiv 20 \pmod{25} \quad (2.8)$$

Пример 3. Пусть n=49, тогда

$$\left[\frac{\mathrm{n}}{3}\right]! = \left[\frac{49}{3}\right]! = 16!.\ 1\cdot2\cdot3\cdot4\cdot5\cdot6\cdot7\cdot8\cdot9\cdot10\cdot11\cdot12\cdot13\cdot14\cdot15\cdot16,$$

и

$$\left[\frac{49}{3}\right]! \equiv 0 \pmod{25}, \quad (2.9)$$

потому что 7·14=2·49.

Из последнего примера видно, что последующие числа вида n^k, где $n \in N$, $k \in N$, $n \geq 7$, $k \geq 2$, будут иметь результат:

$$\left[\frac{\boldsymbol{n}^{\boldsymbol{k}}}{3}\right]! \equiv 0 \pmod{n^k}, \quad (2.10)$$

и вследствие этого факта будут подчиняться условию (2.6), и соответственно, не будут являться простыми числами.

Теорема доказана.

Мы убедились, что теорема индийских математиков Агравала, Кайаны и Саксены 1.71 равнозначна малой теореме Ферма и поэтому не дает гарантированной простоты проверяемого числа и потому не эффективен.

Список литературы

1. Agrawal M., Kayal N., Saxsena N. – PRIMES is in P. Preprint, August 2002. – С. 48-52.

2. Alford W.R., Grenville A., Pomerance C. There are infinitely many Carmichael nambers. // Ann. Math. 1994. V. 140.

3. Ingham A.E. The Distributhion of Prime Numbers. Stechert-Hafner Service Agency. – New York and London, 1964. – С. 7-11.

4. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии. МЦНМО, – М., 2003. – С. 52-54.

5. Серпинский В. Что мы знаем и чего не знаем о простых числах. – М.–Л.: Гос. изд-во физико-математической литературы, 1963.– С. 51-53.

6. Трост Э. Простые числа. – М.: Гос. изд-во физико-математической литературы, 1959. – С. 30-32.