ПРОВЕРКА ЧИСЕЛ НА ПРОСТОТУ: ПОЛИНОМИАЛЬНЫЙ АЛГОРИТМ*

И. В. Агафонова

ivagafonova@home.eltel.net

3 октября 2009 г.

В 2002 г. индийским математиком Агравалом (Agrawal) и двумя его студентами Кайялом (Kayal) и Саксеной (Saxena) был предложен произведший ошеломляющее впечатление алгоритм проверки простоты чисел [1]. Этот алгоритм, формально опубликованный в 2004 г. [2], стали называть алгоритмом AKS. Авторы оригинально модифицировали существующие тесты и создали первый алгоритм, который удовлетворяет одновременно трём требованиям:

- детерминированный — всегда находит корректный ответ;
- безусловный — не опирается на какие-либо недоказанные гипотезы, такие, как обобщённая гипотеза Римана[1)];
- полиномиальный — асимптотическое время выполнения полиномиально.

Большая часть идей, используемых в алгоритме AKS, была в широком обращении, но до указанных авторов никто на их основе не преуспел в построении алгоритма с такими свойствами. Более ранние тесты на простоту могли удовлетворять двум из этих свойств, но не всем трём.

Из предшествующих детерминированных алгоритмов быстрейшие (например, Адлемана-Померанса-Румели, см. [3]) имеют время выполнения порядка $O\big((\log n)^{c \log\log n}\big)$[2)]. Это экспоненциальное время, однако степень $c \log\log n$ стремится к бесконечности с ростом $\log n$ довольно медленно. Так, при $d < 10^{38}$ значение $\log\log d$ не превышает 7.

---

*Семинар по дискретному гармоническому анализу и геометрическому моделированию «DHA & CAGD»: `http://www.dha.spb.ru/`

1) Обобщённая гипотеза Римана: комплексные нули всех L-функций Дирихле, расположенные в полосе $0 < Re\ s < 1$, лежат на прямой $Re\ s = 1/2$.

2) Здесь и далее log будет означать логарифм по основанию 2.

Классические основания алгоритма AKS

При описании алгоритма и при доказательстве его корректности постоянно используются сравнения и их свойства. Эта тема прекрасно изложена в известном учебнике [4].

1. Теоремы Эйлера и Ферма:
   - Если $m > 1$ и НОД$(a, m) = 1$, то $a^{\varphi(m)} \equiv 1 \pmod m$, где $\varphi(r)$ — функция Эйлера (теорема Эйлера).
   - Если p — простое число, то $a^p \equiv a \pmod p$ (малая теорема Ферма).

Из последней теоремы при простом p получаем $(x + y)^p \equiv x + y \pmod p$ и $x^p + y^p \equiv x + y \pmod p$, откуда следует примечательное тождество

$$(x + y)^p \equiv x^p + y^p \pmod p,$$

иногда называемое детской биномиальной теоремой.

2. Критерий простоты:

Если a и n взаимно просты, то тождество

$$(x + a)^n \equiv (x^n + a) \pmod n \tag{1}$$

выполняется тогда и только тогда, когда n — простое число.

Сравнение понимается так: все коэффициенты многочлена $(x+a)^n-(x^n+a)$ кратны n.

Сразу заметим, что если это тождество непосредственно использовать для проверки простоты, то алгоритм тестирования будет иметь время выполнения порядка $O(n)$ (по числу проверяемых коэффициентов полинома), то есть будет экспоненциальным.

Приведём доказательство тождества (1), опираясь на замечательное свойство биномиальных коэффициентов: $C_n^k \equiv 0 \pmod n$ для всех $k \in 1 : n - 1$ тогда и только тогда, когда n — простое.

> Доказательство этого свойства можно провести, используя представление $C_n^k = \frac{n!}{k!(n-k)!}$. Эта дробь — целое число. При простом n и $k \in$ $\in 1 : n - 1$ её числитель содержит множитель n, а знаменатель — нет, так что множитель n несократим и является делителем C_n^k.
>
> Обратно, пусть $C_n^k \equiv 0 \pmod n$ для всех $k \in 1 : n-1$. Предположим, что n составное, и пусть простое число p входит в разложение n в степени k, то есть n делится на p^k и не делится на p^{k+1}. Тогда биномиальный коэффициент $C_n^p = \frac{n(n-1)\cdots(n-p+1)}{p!}$ не может делиться на p^k. (Это очевидно: в числителе идут p сомножителей подряд, первый делится на p, тогда остальные — нет). Значит, он не делится и на n.

По биномиальной формуле,

$$(x+a)^n = x^n + a^n + \sum_{k=1}^{n-1} C_n^k \, x^{n-k} \, a^k = x^n + a + (a^n - a) + \sum_{k=1}^{n-1} C_n^k \, x^{n-k} \, a^k,$$

так что

$$(x+a)^n - (x^n + a) = (a^n - a) + \sum_{k=1}^{n-1} C_n^k \, x^{n-k} \, a^k. \tag{2}$$

Пусть n простое. Тогда по малой теореме Ферма и по свойству биномиальных коэффициентов оба слагаемых правой части делятся на n.

Обратно, пусть (1) выполняется, то есть выполняется (2). Тогда все коэффициенты многочлена в правой части (2) должны быть кратны n. Так как a и n взаимно просты, то это значит, что все C_n^k при $k \in 1 : n-1$ кратны n, то есть, по свойству биномиальных коэффициентов, число n — простое.

3. Некоторые свойства порядка числа по модулю:

Порядок (или *показатель*) числа n по модулю r, обозначаемый здесь как $order_r(n)$ — это минимальное число d такое, что $n^d \equiv 1 \pmod r$. Число r взаимно просто с n, иначе порядок не определен. Нетрудно проверить, что:

- все вычеты n^i по $\mod r$ при различных $i \leqslant order_r(n)$ различны (действительно, если $n^i \equiv n^j \pmod r$ при $i > j$, то $n^{i-j} \equiv 1 \pmod r$, чего не может быть при $i - j < order_r(n)$);
- $r > order_r(n)$ (вытекает из теоремы Эйлера, так как $r > \varphi(r)$).

4. Сравнения по двум модулям:

Сравнение вида

$$a(x) \equiv b(x) \pmod{(h(x), n)}$$

означает следующее: для многочленов $a(x)$ и $b(x)$ из $Z[x]$ (кольца многочленов от x с целыми коэффициентами) найдётся многочлен $q(x) \in Z[x]$ такой, что все коэффициенты многочлена $a(x) - b(x) - h(x)\,q(x)$ кратны n.

В частности, при $h(x) \equiv 0$ будем иметь $a(x) \equiv b(x) \pmod n$, как рассматривалось выше.

AKS: описание и оценка сложности алгоритма

Сразу из (1) вытекает следующее необходимое условие простоты:
Если n просто, то для любого целого $r > 0$ и любого целого a, $0 < a < n$, выполняется сравнение

$$(x + a)^n \equiv (x^n + a) \pmod{x^r - 1, n}. \tag{3}$$

К сожалению, обратное утверждение неверно. Однако желаемый результат был достигнут Агравалом, Кайялом и Саксеной при использовании некоторого определённого r и некоторого множества значений для a. Достаточные условия простоты числа n были сведены к выполнению требований:

(i) значение r должно быть таким, что $order_r(n) > L$, где L зависит от n;

(ii) соотношение (3) выполняется для любого целого a из интервала $[1, A]$, где A зависит от n и r.

(Иногда вместо $[1, A]$ указывают интервал $[0, A]$. Это то же самое, так как при $a = 0$ условие (3) выполнено.)

В разных изложениях алгоритма, в том числе и разных авторских, значения L и A несколько различаются. Мы будем проводить все доказательства и расчёты для принятых в [5] значений

$$L = 4 \log^2 n, \quad A = 2\sqrt{r} \log n.$$

ТЕОРЕМА (AKS). *Если существует r, удовлетворяющее (i), при котором для всех a, удовлетворяющих (ii), выполняется условие* (3), *то n либо простое, либо степень простого.*

На основе этой теоремы, доказательсто которой будет приведено ниже, построен алгоритм, схема которого помещена в следующую таблицу. Используется обозначение $\tilde{O}$ — так называемое «мягкое O»:

$$\tilde{O}(y) = O\big(y(\log y)^{O(1)}\big).$$

Алгоритм AKS. На входе — нечётное число n.	
Шаги алгоритма	Оценка числа битовых операций
Определить, будет ли n точной степенью целого числа, $n=m^k$ для какого-то $k>1$. Если да, возврат СОСТАВНОЕ.	$\tilde{O}(\log^3 n)$ (и даже $\tilde{O}(\log n)$, если применять алгоритм [6]).
Если n — не точная степень, то	
Найти такое целое r, что $order_r(n) > L$. Для этого надо вычислять $n^j \pmod q$ при $j = 1, 2, \ldots, \lfloor L \rfloor$ при каждом целом $q > L$, пока не найдётся первое q, для которого ни один из этих $n^j \pmod q$ не равен 1. После этого принять $r = q$.	$O(r \cdot \log^2 n \cdot \log^2 r)$, где r оценивает количество обращений к q, а $O(\log^2 n \cdot \log^2 r)$ оценивает при фиксированном q трудоёмкость вычисления $n^j \pmod q$ с учетом $q \leqslant r$ и $j \leqslant 4\log^3 n$.
Проверить основное соотношение $$(x+a)^n \equiv (x^n + a) \pmod{x^r - 1, n}$$ для каждого целого $a \in [1, 2\sqrt{r}\log n]$. Если найдётся a, для которого оно выполнится, возврат СОСТАВНОЕ.	$\tilde{O}(r^{\frac{3}{2}} \log^3 n)$. Наиболее трудоёмкая часть: для каждого a нужно $r\,\tilde{O}(\log^2 n)$ битовых операций при использовании бинарного возведения в степень и быстрого преобразования Фурье.
Если не вышли из алгоритма раньше, возврат ПРОСТОЕ.	

В изложенном алгоритме опущены не имеющие принципиального значения часто включаемых детали, такие, как предварительная проверка n на наличие малых простых делителей или досрочный выход, если на шаге поиска числа r обнаружится какой-либо собственный множитель числа n.

Оценки в таблице приведены в предположении, что для умножения целых чисел применяется быстрейший из известных алгоритмов — алгоритм Шёнхаге-Штрассена (см., например, [7]), который на перемножение двух чисел длины $\log n$ тратит $\tilde{O}(\log n)$ битовых операций.

Для завершения оценки сложности алгоритма необходимо оценить размер числа r. Как отмечалось выше, $r > order_r(n) > L = 4\log^2 n$. Из последнего шага приведённого выше алгоритма, где в оценке сложности фигурирует $r^{\frac{3}{2}}$, видно, что алгоритм AKS требует не менее $\tilde{O}(\log^6 n)$ битовых операций, и это нижняя оценка сложности алгоритма. Верхняя, более важная оценка получается на основе следующей леммы.

ЛЕММА. *Существует число* $r \leqslant \lceil 16\log^5 n \rceil$, *удовлетворяющее* (i).

Доказательство. Обозначим $K = \lceil L \rceil = \lceil 4\log^2 n \rceil$ и рассмотрим произведение $P = n \cdot \prod_{j=1}^{K}(n^j - 1)$. Число P делится на некоторое r тогда и только тогда, когда либо n делится на r, либо при каком-то j выполняется $n^j \equiv 1 \pmod r$ (последнее возможно лишь при $order_r n \leqslant K$). Оценим величину

$$P = n \cdot \prod_{j=1}^{K}(n^j - 1) < n \cdot \prod_{j=1}^{K} n^j = \prod_{j=2}^{K+1} n^j = n^{\sum_{j=2}^{K+1} j}.$$

Так как $\sum_{j=2}^{K+1} j = \frac{(K+3)K}{2} < K^2$ (это неравенство выполнено, поскольку $n \geqslant 2$ и, значит, $K \geqslant 4$), то $P < n^{K^2} \leqslant n^{16\log^4 n} = 2^{16\log^5 n}$.

Доказано [8], что при $T \geqslant 9$ наименьшее общее кратное всех чисел от 1 до T, которое далее обозначается как НОК$(1, 2, ..., T)$ или просто НОК(T), будет больше либо равно 2^T (на самом деле неравенство верно при $T \geqslant 7$, при $T = 7$ и при $T = 8$ оно проверяется непосредственно)[3]. Возьмём $T = \lceil 16\log^5 n \rceil$. Так как $T \geqslant 16\log^5 n \geqslant 16\log^5 2 = 16$, то условие $T \geqslant 7$ выполнено. Значит, $P <$ НОК(T), так что среди чисел от 1 до T есть r, на которое P не делится.

Возможны два случая: либо НОД$(n, r) = 1$, и тогда r — то самое, о существовании которого говорит лемма, либо НОД$(n, r) > 1$. В последнем случае заметим, что P делится на n и не делится на r, значит, делится на НОД(n, r) и не делится на $s = \frac{r}{\text{НОД}(n,r)}$. Число s и будет требуемым, так как НОД$(s, n) = 1$. □

Эта лемма дает оценку $r = O(\log^5 n)$ и общую оценку числа битовых операций $\tilde{O}(r^{\frac{3}{2}} \log^3 n) = \tilde{O}(\log^{10.5} n)$ (по наиболее трудоёмкому последнему шагу).

Корректность алгоритма AKS

Алгоритм верно определяет простые и составные числа, если верна приведённая выше теорема AKS. Доказательство теоремы будет проводиться от противного. Делается предположение, что при r, удовлетворяющем (i) и (ii), число n имеет простой делитель p, но не является его степенью. Тогда сравнение (3) верно и по модулю $(x^r - 1, p)$.

Основная идея: вместо кольца $F_p[x]/(x^r - 1)$ рассматривают поле

$$F = F_p[x]/(h),$$

где $h = h(x)$ — неприводимый делитель $x^r - 1$ над полем F_p, отличный от $x - 1$. Оценивают число многочленов этого поля, для которых выполняется соотношение вида (3), и приходят к противоречию.

К некоторым пунктам доказательства, относящимся к свойствам многочленов над конечными полями, имеются пояснения в Приложении 2.

[3] Доказательство этого утверждения представляет интерес и полностью приведено в Приложении 1.

Доказательство теоремы AKS.

Предположим, что условия теоремы выполнены, то есть нашлось r такое, что $order_r(n) > L$ и для целого $a \in [1, A]$ имеет место сравнение

$$(x+a)^n \equiv (x^n + a) \pmod{x^r - 1, n},$$

но n — не степень простого и имеет простой делитель p.

Введем два множества:

$$U = \{m : (x+a)^m \equiv (x^m + a) \pmod{x^r - 1, p} \quad \forall a : 1 \leqslant a \leqslant 2\sqrt{r}\log n\},$$

$$V = \{g(x) : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p} \quad m \in U\}.$$

Очевидно, что 1, p и n принадлежат U[4)] и что $x + a \in V$. Более того, непосредственно видно, что оба множества U и V замкнуты относительно умножения и, следовательно, бесконечны.

Проверка замкнутости:

- Для множества U имеем

$$(x+a)^{m_1} \equiv (x^{m_1} + a) \pmod{x^r - 1, p},$$

$$(y+a)^{m_2} \equiv (y^{m_2} + a) \pmod{x^r - 1, p}.$$

  Первое сравнение возведём в степень m_2 и воспользуемся вторым сравнением.

$$(x+a)^{m_1 \cdot m_2} \equiv (x^{m_1} + a)^{m_2} \pmod{x^r - 1, p} \equiv$$

$$\equiv (x^{m_1 \cdot m_2} + a) \pmod{x^r - 1, p}.$$

- Для множества V имеем

$$g(x)^m \equiv g(x^m) \pmod{x^r - 1, p} \quad m \in U\},$$

$$h(x)^m \equiv h(x^m) \pmod{x^r - 1, p} \quad m \in U\}$$

  и просто перемножаем сравнения.

[4)] $n \in U$, так как выполнено (3) и так как p — делитель n; $p \in U$, потому что p простое и для него выполняется (3).

В частности, отметим тот факт, что $n^i p^j \in U$ при всех целых неотрицательных i, j.

Определим теперь два конечных множества

$$U_0 = \{m \pmod r), m \in U\},$$

$$V_0 = \{g(x) \pmod{h(x), p}), m \in U\},$$

где $h(x)$ — минимальный многочлен примитивного корня ζ степени r из 1 над полем F_p (см. Приложение 2).

Оценим размер этих двух множеств.

Обозначим $t = |U_0|$ — число элементов множества U_0. Так как элементы U_0 — вычеты по модулю r, то $t \leqslant r$.

Множество U содержит все степени n, среди них по свойству порядка первые $order_r(n)$ степеней различны по модулю r. Тогда $t \geqslant order_r(n) > L$.

Обозначим $T = |V_0|$. Так как элементы V_0 — полиномы по модулю $h(x)$ с коэффициентами из F_p, степень которых, очевидно, меньше степени полинома $h(x)$, не превосходящей $r-1$, то $T \leqslant p^{r-1}$.

Нижнюю границу T определить немного сложнее .

Рассмотрим два различных полинома $f(x), g(x)$ из V степени меньше t, и пусть $f(x) = g(x)$ в V_0, то есть $f(x) \equiv g(x) \pmod{h(x), p}$.

Имеем

$$f(x^m) \equiv f(x)^m \equiv g(x)^m \equiv g(x^m) \pmod{h(x), p} \text{ при всех } m \in U.$$

Тогда это сравнение верно и при всех $m \in U_0$.[5)] Поэтому полином $f(y) - g(y)$ имеет не менее $|U_0| = t$ корней вида x^m в поле F, причём различных (см. Приложение 2). Так как степень полинома $f(y) - g(y)$ меньше t и $f(y) \neq g(y)$, это невозможно. Это показывает, что все различные полиномы степени меньше t в V отображаются в различные элементы в V_0.

Завершают оценку снизу для T следующие рассуждения.

- Множество V содержит все полиномы $(x+a)$ при целых $a \in [0, A]$, то есть имеет не менее $\lfloor A \rfloor + 1$ полиномов степени 1. Кроме того, V замкнуто относительно умножения.

- Число различных полиномов степени меньшей, чем t, в множестве V больше, чем $n^{2\sqrt{t}} (= 2^{2\sqrt{t}\log n} = 2^A)$.

  Докажем это. Так как $r \geqslant t$, мы можем рассмотреть множество M из каких-либо $\lfloor A \rfloor + 1$ полиномов 1-й степени из V. Число

[5)] Доказательство. Так как $x^r = 1$ в поле $F = F_p[x]/(h)$, то $f(x^{m+kr}) = f(x^m)$ в F.

его элементов обозначим $m = |M| = \lfloor A \rfloor + 1$. Так как $4\log^2 n < t$, то $4t\log^2 n < t^2$ и, соответственно, $A = 2\sqrt{t}\log n < t$, откуда $m \leqslant t$. В таком случае любое собственное подмножество множества M состоит из менее чем t элементов, самое большее из $t-1$, и произведение этих элементов дает многочлен степени меньше t. Таких подмножеств, как известно, имеется $2^m - 2$. Значит, мы можем составить не менее $2^m - 2 \geqslant 2^{2\sqrt{t}\log n} - 2 = n^{2\sqrt{t}} - 2$ различных многочленов степени меньше t из различных элементов M.

Не хватает ещё двух полиномов. Вспомним, что n составное и не степень простого, так что $n \geqslant 6$ и, соответственно, $4\log^2 n > 26$. Из неравенств $4\log^2 n < t$ и $t \leqslant r$ заключаем, что и t, и r больше 26, так что $m > 10\log n > 25$. Так как полиномы степени меньше t мы можем получать перемножением элементов множества M, которые не обязательно все различны, и так как по крайней мере m полиномов 2-й степени — просто квадраты полиномов 1-й степени, то можно быть уверенными, что из элементов множества M получаются больше $n^{2\sqrt{t}}$ различных многочленов степени меньше t. Так как все они входят и в V, то и для V верна эта же оценка.

- Следовательно, и $|V_0| > n^{2\sqrt{t}}$.

Объединяя верхнюю и нижнюю оценки, получаем двойное неравенство

$$n^{2\sqrt{t}} < T \leqslant p^{r-1}.$$

Выведем соотношение, связывающее n и его простой делитель p.

- Так как множество U_0 содержит t элементов и $n^i\,p^j \pmod r \in U_0$, то существуют две несовпадающие пары (i,j) и (k,l), где $i,j,k,l \leqslant \sqrt{t}$, такие, что $n^i\,p^j \equiv n^k\,p^l \pmod r$.

  Поясним это утверждение. Количество всех произведений вида $n^i\,p^j$ при $0 \leqslant i,j \leqslant \sqrt{t}$ составляет $(1 + \lfloor\sqrt{t}\rfloor)^2 = 1 + 2\lfloor\sqrt{t}\rfloor + (\lfloor\sqrt{t}\rfloor)^2$. Так как можно представить $\lfloor\sqrt{t}\rfloor = \sqrt{t} - \alpha$, где $\alpha \in [0,1)$, то это выражение равно $1 + 2\sqrt{t} - 2\alpha + (\sqrt{t}-\alpha)^2 = 1 + 2\sqrt{t} - 2\alpha + t - 2\alpha\sqrt{t} + \alpha^2 = t + 2\sqrt{t}\,(1-\alpha) + (1-\alpha)^2 > t$. Таким образом, число всех произведений такого вида больше, чем t — число элементов множества U_0. Значит, какие-то из них отвечают одному и тому же элементу U_0, то есть совпадают по модулю r.

- Возьмём $g(x) \in V_0$. Имеем

$$g(x)^{n^i\,p^j} = g(x^{n^i\,p^j}) = g(x^{n^k\,p^l}) = g(x)^{n^k\,p^l} \pmod{p, h(x)}.$$

Второй знак равенства в этой цепочке опирается на то, что $x^r = 1$ в поле F, так что для любых чисел m_1 и m_2 из U, сравнимых по модулю r, будет $x^{m_1} = x^{m_2}$ в поле F.

- Поэтому каждый многочлен $g(x) \in V_0$ есть корень полинома $y^{n^i p^j} - y^{n^k p^l}$ над полем F.
- Так как по нашему выбору получаем $n^i p^j \leqslant n^{\sqrt{t}} p^{\sqrt{t}} \leqslant n^{\sqrt{t}} n^{\sqrt{t}} = n^{2\sqrt{t}}$ и $n^k p^l \leqslant n^{2\sqrt{t}}$, а множество V_0 содержит $T > n^{2\sqrt{t}}$ элементов (корней полинома в поле F), то этот полином — тождественный 0.
- Отсюда $n^i p^j = n^k p^l$.
- Так как p — простое и делит n, то это значит, что $n = p^c$ при некотором $c > 0$.

Полученное выражение $n = p^c$ противоречит сделанному предположению, что n — не степень простого числа. □

Развитие алгоритма AKS

Степень 10.5 является слишком высокой для практически полезного алгоритма. Оценку сложности алгоритма можно улучшить до $\tilde{O}(\log^6 n)$, сделав некоторые известные, но недоказуемые допущения. Кроме того, классики в этой области Ленстра (Lenstra) и Померанс (Pomerance) предложили корректную вариацию алгоритма AKS [9] сложности $\tilde{O}(\log^6 n)$. Вместо полинома $x^r - 1$ в этой версии используется другой унитарный полином $f(x)$ степени $d > \log^2 n$ со свойством $f(x^n) \equiv 0 \pmod{f(x)}$, удовлетворяющий дополнительно некоторым условиям.

Алгоритм AKS и его модификации на практике пока не могут конкурировать по удобству использования и времени выполнения с другими известными алгоритмами.

Приложение 1.

Приведённая здесь лемма, на которую нередко ссылаются, как на самостоятельный результат, не имеет отдельной формулировки в [8], она вычленена из доказательства одной из имеющихся в [8] теорем.

ЛЕММА. *При $T \geqslant 9$ наименьшее общее кратное всех чисел от 1 до T больше либо равно 2^T.*

Доказательство. Рассмотрим при $m \in 1 : n$ интеграл

$$S(n,m) = \int_0^1 x^{m-1}\,(1-x)^{n-m}\,dx = (\text{бином Ньютона}) =$$
$$= \int_0^1 x^{m-1} \sum_{k=0}^{n-m} C_{n-m}^k (-1)^k\, x^k\, dx =$$
$$= \sum_{k=0}^{n-m} C_{n-m}^k (-1)^k \int_0^1 x^{m-1+k}\,dx = \sum_{k=0}^{n-m} C_{n-m}^k (-1)^k\, \frac{1}{m+k}\,.$$

Очевидно, что НОК(n), наименьшее общее кратное всех чисел от 1 до n, делится на $m+k$ при всех k от 0 до $n-m$, так что число НОК$(n) \cdot S(n.m)$ — целое. С другой стороны,

$$S(n,m) = (\text{по частям}) = \frac{1}{m}\int_0^1 (1-x)^{n-m}\,dx^m =$$
$$= \frac{1}{m}\int_0^1 x^m\,(n-m)\,(1-x)^{n-m-1}\,dx =$$
$$= \frac{n-m}{m}\int_0^1 x^m\,(1-x)^{n-m-1}\,dx = (\text{снова по частям}) =$$
$$= \frac{(n-m)(n-m-1)}{m(m+1)}\int_0^1 x^{m+1}\,(1-x)^{n-m-2}\,dx = (\text{и так далее}) =$$
$$= \frac{(n-m)(n-m-1)\cdots 1}{m(m+1)\cdots(n-1)}\int_0^1 x^{n-1}\,dx = \frac{(n-m)!}{m(m+1)\cdots(n-1)\,n} =$$
$$= \frac{(n-m)!\,(m-1)!}{n!} = \frac{1}{m\,C_n^m}\,.$$

Возьмем $n = 2N, m = N$. Так как число НОК$(2N) \cdot S(2N,N) = \frac{\text{НОК}(2N)}{NC_{2N}^N}$, как было замечено выше, целое, то НОК$(2N)$ делится на NC_{2N}^N. Тогда $(2N+1)\,C_{2N}^N$ также делится на NC_{2N}^N.

Возьмем теперь $n = 2N+1, m = N+1$. Аналогично предыдущему, число НОК$(2N+1)$ делится на $(N+1)\,C_{2N+1}^{N+1}$.

Учитывая легко проверяемое равенство $(2N+1)\,C_{2N}^N = (N+1)\,C_{2N+1}^{N+1}$, получаем, что НОК$(2N+1)$ делится на $(2N+1)\,C_{2N}^N$. Сравнивая делители $(2N+1)\,C_{2N}^N$ и NC_{2N}^N и учитывая, что $2N+1$ и N взаимно просты[6)], получаем, что НОК$(2N+1)$ должно делиться на $N(2N-1)\,C_{2N}^N$. Тогда НОК$(2N+1) \geqslant N(2N+1)\,C_{2N}^N$.

[6)] Известное свойство наибольшего общего делителя: для любого целого m выполняется равенство НОД$(a+mb,b) = $ НОД(a,b).

Так как C_{2N}^N — наибольшее из $2N+1$ слагаемых биномиального разложения $(1+1)^{2N}$, то $(2N+1)\,C_{2N}^N \geqslant (1+1)^{2N} = 4^N$. Приходим к неравенству

$$\text{НОК}(2N+1) \geqslant N \cdot 4^N. \tag{4}$$

Отсюда при $N \geqslant 2$ имеем $\text{НОК}(2N+1) \geqslant 2^{2N+1}$. Кроме того,

$$\text{НОК}(2N+2) \geqslant \text{НОК}(2N+1) \geqslant (\text{по неравенству (4)}) \geqslant N \cdot 4^N,$$

так что при $N \geqslant 4$ выполнится $\text{НОК}(2N+2) \geqslant 2^{2N+2}$. Таким образом, и при чётных, и при нечётных $N \geqslant 9$ имеет место неравенство

$$\text{НОК}(N) \geqslant 2^N.$$

$\square$

Приложение 2.

В этом приложении для справки приведены некоторые алгебраические определения и результаты, используемые при доказательстве теоремы AKS.

О фактор-кольце $F_p[x]/(h)$

Здесь $F_p[x]$, как обычно, означает кольцо многочленов с коэффициентами из конечного поля F_p, содержащего p элементов (p — простое число).

Фактор-кольцо $F_p[x]/(h)$ строится по произвольному ненулевому многочлену $h(x) \in F_p[x]$ и состоит из классов вычетов $f + (h) = \{f + gh, g \in F_p[x]\}$, $f \in F_p[x]$ с операциями, определяемыми следующим образом:

$$(f + (h)) + (\varphi + (h)) = (f + \varphi) + (h),$$

$$(f + (h))(\varphi + (h)) = (f\varphi) + (h).$$

В каждом классе вычетов имеется единственный многочлен r степени меньшей, чем $\deg h$ (это остаток при делении на h), так что число элементов множества $F_p[x]/(h)$ равно числу многочленов степени, меньшей $\deg h$, в кольце $F_p[x]$, то есть $p^{\deg h}$.

Если многочлен $h(x)$ неприводим над F_p, кольцо $F_p[x]/(h)$ является полем.

О поле $F_p(\zeta)$

Пусть r - натуральное число, не делящееся на простое число p.

Через $F_p^{(r)}$ обозначим поле разложения многочлена $x^r - 1$ над F_p, то есть наименьшее поле, содержащее F_p и все r корней ζ_i степени r из 1. Множество этих корней образует циклическую группу, так что $\zeta_i = \zeta^i$, где ζ — образующий элемент этой группы, называемый примитивным корнем степени r из 1 над полем F_p.

Поле $F_p^{(r)}$ совпадает с $F_p(\zeta)$ — простым алгебраическим расширением поля F_p.

О выборе $h(x)$ и многочленах x^i в поле $F_p[x]/(h)$

Выбор делается при описанных выше r, p и ζ.

В качестве $h(x)$ берётся минимальный многочлен элемента ζ над полем F_p. Тогда:

- $h(x)$ неприводим в кольце $F_p[x]$;
- $h(x)$ является делителем любого другого многочлена с корнем ζ, в частности, многочлена $x^r - 1$;
- поле $F_p[x]/(h)$ изоморфно полю $F_p(\zeta)$.

Изоморфизм $\psi : F_p[x]/(h) \to F_p(\zeta)$ можно задать как $\psi(f) = f(\zeta)$. Тогда при $f = x$ имеем $\psi(x) = \zeta$. Вследствие изоморфизма многочлен x является примитивным корнем степени r из 1 в $F_p[x]/(h)$. Следовательно, степени x^i при $i \in 0 : r - 1$ различны в поле $F_p[x]/(h)$.

ЛИТЕРАТУРА

1. Agrawal M., Kayal N., Saxena N., *PRIMES is in P* //
`http://www.cse.iitk.ac.in/manindra/algebra/primality_original.pdf`

2. Agrawal M., Kayal N., Saxena N., *PRIMES is in P* // Annals of Mathematics. 2004. V. 160. No. 2 P. 781–793.

3. Василенко О. Н. *Теоретико-числовые алгоритмы в криптографии.* М.: МЦНМО, 2003. 328 с.

4. Виноградов И. М. *Основы теории чисел.* М.: Наука, 1965. 172 с.

5. Agrawal M. *Primality tests based on Fermat's little theorem* //Proceedings of ICDCN'2006. P. 288–293.

6. Bernstein D. *Detecting perfect powers in essentially linear time* // Mathematics on Computation. 1998. V. 67. No. 223. P. 1253–1283.

7. Ахо А., Хопкрофт Дж., Ульман Дж. *Построение и анализ вычислительных алгоритмов.* М.: Мир, 1979. 536 с.

8. Nair M. *On Chebyshev-type inequalities for primes* //American Mathematical Monthly. 1982. V. 89. No. 2. P. 126–129.

9. Lenstra H., Pomerance Jr. and C. *Primality testing with Gaussian periods.* // Preprint. 2005.