Лекция по дискретной математике

15 апреля 2019

$\pi(n) \sim n/log(n)$
Сколько простых чисел от 1 до n?
log(n)-кол-во цифр
$\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$
$e - \forall$ от 2 до $\varphi(N) - 2(e; \varphi(n)) = 1$
d-Находится, как решение $\mathrm{ed}_{\varphi(n)} \equiv 1$
Почему работает?
т.е. $m_N^{ed} \equiv m$
Проверка:
$ed \equiv 1 \Longrightarrow ed = 1 + k\varphi(N) \Longrightarrow m_N^{ed} \equiv m_N^{1+k\varphi(N)} \equiv m(m^{\varphi(n)})_N^k \equiv m * 1_N^k \equiv m$
Пример:
$p = 5\ q = 7\ N = 35\ \varphi(W) = 4 * 6 = 24$
$e = 5\ d = 19\ 5 * 5_{24} = 1$
Задача:
1) $e = 7\ d =?\ 7d_{24} = 1$
N,e-откр. ключ
N,d-прив.кл.
$(m^e)_N^d \equiv m$
Шифрование: $\bar{m} = m^e mod N$
Расшифрование: $m = \bar{m}^d mod N$
в д-ве было $m_N^{\varphi(N)} \equiv 1$ верно если $(N, m) = 1$
Теор.Эйлера
1) Можно д-ть иначе, идея $N = pq$
$\varphi(N) = (p-1)(q-1)$
2) Если $(m, N) \neq 1 \Longrightarrow (m, N) = p$ или $q \Longrightarrow$ знач. $\varphi(N) \Longrightarrow$ знач. d
Электронная подпись
m-сообщение, хочет д-ть, что это его сообщение
(N, d)-закр.ключ
Эл.Подпись: $m^d mod N = \bar{m}$
Проверка ЭП: $m = \bar{m}^e mod N$
$[hash(m)]^d \mod N$-ср-ния сжимает биты
Как убедиться, что никто не подлжолил открытый ключ?
Откр. ключ тоже подписывают (центр сертификации)
Многочлены

Выражение вида $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 x + a_0$
a_i-эл-т НОТА $(\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}_p)$
x-формальная переменная
$p(x)$-мн-н с переменной "x"
$\deg p(x)$ = степень x при первом ненулевом коэф.
если $a_n \neq 0 \Longrightarrow \deg(a_n x^n + \cdots = n$
$deg0 = -\infty$ (нулевой многочлен)
Пример: $deg(x^2 + 5) = 2$
$deg(o_x^4 + o_x^2 + x - 5) = 1$
$deg(7) = 0$
Действия с многочленами:

- $(x^3 + x) + (x^3 - x^2 - x - 1) = 2x^3 - x^2 - 1$
- $(x^2 + 2x + 5)(x - 1) = x^3 + x^2 + 3x - 5$

В общем виде:
Умножение:
$(a_n x^p + ... + a_0)(b_m x^m + ... + b_0) = C_{n+m}x^{n+m} + ... + C_0$
$C_i = a_0 b_i + a_i b_{i+1} + a_i b_{i+2} + ... + a_i b_0 = \Sigma_{k=0}^{i} a_k b_{i-k}$
Деление:
$x^2 + 1$ не делится на X т.к. $x^2 + 1 = p(x) * x$
Утв. deg $p(x)q(x) = degp(x) + degq(x)$
Д-во очевидно
Деление с остатком:
Делитель: p(X),q(x)
Деление $p(x) = q(x)\varphi(x) + \Psi(x^i)$ при этом $degr(x) = degq(x^i)$
Утв.: Деление с остатком единственно
Д-во:
$\sigma p(x) = q(x)\varphi_1(x) + r_1(x)$
$p(x) = q(x)\varphi_2(x) + r_2(x)$
$0 = q(x)(\varphi_1(x) - \varphi_2(x)) + (r_1(x) - r_2(x) \neq 0 = x^n$
Пример:
Частное: $2x^2 + 5x + 3$
Делитель: $3x + 1$
Остаток: $14/9$
Итог: $2/3x + 13/9$
$2x^2 + 5x + 3 = (3x + 1)(1/3x + 13/9) + 14/9$
Замечание: если $p(x), q(x) \in Z[x]$ целый коэф.
если $q(x) - x^n + ...$-унит пр.
Тогда при делении результата $(\varphi(x) + \psi(x) \in \mathbb{Z}[x]$
Корни мн-на:
x_0-корень $p[x]$,если $p(x_0) = 0$
Деление на $x - \varphi$
$\supset p(x) = (x - \varphi)q(x) + r$
Подставим вместо x a: $\supset x = a$

Д-во:
$p(a) = (a-a)\varphi(x) + \psi \Longrightarrow p(a) = r$ т.Безу
Значение мн-на при $x = a$ равно остатку от деления его на $x - a$
Следствие: $p(x); x - a \Leftrightarrow p(a) = 0$ а-корень
Рассуждение:
$\sqcup$ есть мн-н $p(x) \sqcup$ х-корень $\Longrightarrow p(x) = (x - x_1 p_1(x)$
$\sqcup$ x_2-корень $p_1(x) \Longrightarrow p(x) = (x - x_1)(x - x_2)p_2(x)$ и т.д.
$\Longrightarrow p(x) = (x - x_1)(x - x_2 ... (x - x_n p_x(x)$ нет корней
$degp(x) \geqslant k$ $deg = 0$
Корни р:-это корень р
Итого корней у мн-на $\geqslant degp(x)$ если $p(a) \neq 0$
Опр.: В общем случае $p(x) = (x - x_1)^k ... (x - x_m)^{km} q(x)$
x_i-корень p_i кратности k
Утв:$\sqcup$ $degp \leqslant r \sqcup p(a_1) = q(a_1)$ т.е совпадает в n+1 точек
$\sqcup$ $degp \leqslant np(q_n + 1) < (a_n + 1)$
Тогда: $p(x) = q(x)$
Д-во: $\sqcup$ $p(x) = p(x) - q(x)$
$degr(x) \leqslant n$ $r(a_1) = 0 \Longrightarrow n + 1$ корня $\Longrightarrow r(x) = 0 \Longrightarrow p(x) - q(x)$