О некотором свойстве дискретного логарифма

М.А. Черепнев (Москва)

В заметке предложена формула для дискретного логарифма по модулю степени простого числа и по произвольному основанию. Работа инициирована результатами В.М. Сидельникова.

Для вычислений использовано частное Ферма:

$$F_m(a) = \frac{a^{\lambda(m)} - 1}{m} ,$$

где $m \in N$, $(a, m) = 1$, а $\lambda(m)$ — функция Кармайкла.

Теорема. Пусть p - простое число, $\alpha \in N$, $\alpha \geqslant 2$; $g \in Z$, $(p, g) = 1$; $\gamma \in N$ - степень вхождения p в целое число $F_p(g)$. Тогда, если сравнение $g^x \equiv a \pmod{p^\alpha}$ разрешимо, то

1. При $\alpha \in \{1, ..., \gamma\}$ выполнено: $ord_{p^\alpha} g = ord_p g$, и x есть единственное $\mod ord_p g$ решение сравнения $g^x \equiv a \pmod p$.

2. При $\alpha \geqslant \gamma + 1$, $k = \max\{\gamma + 1,\ \alpha - (\gamma + 1)\}$ выполнено: $ord_{p^\alpha} g = p^{\alpha-(\gamma+1)} ord_p g$, и x есть единственное $\mod p^{\alpha-(\gamma+1)} ord_p g$ решение системы

$$\begin{cases} g^x \equiv a \pmod p \\ x \frac{F_{p^{k-\gamma}}(g)}{p^\gamma} \equiv \frac{F_{p^{k-\gamma}}(a)}{p^\gamma} \pmod{p^{\alpha-(\gamma+1)}}. \end{cases}$$

Замечание. Аналогичная теорема при $p > 2$, $\gamma = 0$ доказана Ю.В. Нестеренко (результат не опубликован).

Список литературы

1. Сидельников В.М. Частные Ферма и логарифмирование в конечном простом поле // Материалы международных научных чтений по аналитической теории чисел и приложениям - 1997 - мех.-мат.

2. Riesel H. Some soluble cases jf the discrete logarithm problem // BIT - 1988. - Vol. 28 - No. 4 - p/ 839-851.

3. Takakazu S., Kiyomichi A. Fermat quotients and the polynomial time discrete log algorithm for anomalous ellptic curves // Commentarii mathematiciuniversitatis sancti pauli - 1998. - Vol. 47 - No. 1 - p. 81 - 91.