ПАЩЕНКО В. П. (Белгород)

# ДВА ПРИЗНАКА ПРИНАДЛЕЖНОСТИ ЧИСЛА К ДАННОМУ ПОКАЗАТЕЛЮ ПО ПРОСТОМУ МОДУЛЮ

Как известно, нахождение показателя, к которому принадлежит число, в большинстве случаев связано с громоздкими выкладками. В этой заметке мы рассмотрим два свойства степенных вычетов, позволяющие в некоторых случаях облегчить отыскание показателей по простому модулю.

**Теорема 1.** Число a по простому модулю $p \neq 2$ принадлежит к нечетному показателю r, тогда и только тогда, когда p—a принадлежит к показателю 2r.

**Доказательство.**

1. Пусть a принадлежит к нечетному показателю r, т. е.

$$a \equiv 1 \pmod{p} \qquad (1),$$

где a и r — натуральные числа.

Тогда $a^{2r} \equiv 1 \pmod{p}$, $p^{2r} - C^1_{2r} p^{2r-1} a + \ldots + a^{2r} \equiv 1 \pmod{p}$, $(p-a)^{2r} \equiv 1 \pmod{p}$.

Предположим, что $(p-a)^n \equiv 1 \pmod{p}$, где

$$n < 2r \qquad (2).$$

Число n может быть или четным, или нечетным.

а) Пусть $n = 2r_1$, $r_1 < r$. В этом случае

$p^{2r_1} - C^1_{2r_1} p^{2r_1-1} a + \ldots + a^{2r_1} \equiv 1 \pmod{p}$, $a^{2r_1} \equiv 1 \pmod{p}$.

Но $2r_1$ не делится на r. Получили противоречие.

б) Пусть n — нечетное натуральное число. Тогда

$p^n - C^1_n p^{n-1} a + \ldots + C^{n-1}_n p a^{n-1} - a^n \equiv 1 \pmod{p}$,

$$a^n \equiv -1 \pmod{p} \qquad (3),$$
$$a^2 \equiv 1 \pmod{p} \qquad (4).$$

Сравнение (4) согласно (1) выполняется, если

$$n = qr \qquad (5),$$

где q — натуральное. Соотношения (2) и (5) возможны одновременно только при $q = 1$, т. е. $n = r$. Итак, имеем $a \equiv -1 \pmod{p}$, что противоречит (1).

2) Пусть p—a принадлежит к показателю 2r, т. е.

$$(p-a)^{2r} \equiv 1 \pmod{p} \qquad (6).$$

В этом случае $(p-a)^{2r} - 1 \equiv 0 \pmod{p}$

$$\left[(p-a)^r - 1\right] \cdot \left[(p-a)^r + 1\right] \equiv 0 \pmod{p}.$$

Тогда выполняется одно из двух сравнений:

$$(p-a)^r \equiv 1 \pmod{p} \qquad (7),$$

$$(p-a)^r \equiv -1 \pmod{p} \qquad (8).$$

Но сравнение (7) противоречит условию (6), следовательно, выполняется сравнение (8), которое мы и рассмотрим.

Показатель r может быть либо четным, либо нечетным:

а) пусть r — нечетное число. Тогда из (8) имеем $p^r - C_r^1 p^{r-1} a + \ldots + a^r \equiv -1 \pmod{p}$, т. е. при четном r $a^r \equiv -1 \pmod{p}$;

б) пусть r — нечетное число. В этом случае из (8) будем иметь $p^r - C_r^1 p^{r-1} a + \ldots + C_r^{r-1} p a^{r-1} - a^r \equiv -1 \pmod{p}$, $-a^r \equiv -1 \pmod{p}$, т. е. при нечетном r $a^r \equiv 1 \pmod{p}$.

Покажем, что r — наименьшее нечетное число, для которого выполняется последнее сравнение. Предположим, что $a^{r_1} \equiv 1 \pmod{p}$, где $r_1 < r$.

В этом случае

$$-a^{r_1} \equiv -1 \pmod{p} \qquad (9)$$

Очевидно, что

$$p^{r_1} - C_{r_1}^1 p^{r_1-1} a + \ldots + C_{r_1}^{r_1-1} p a^{r_1-1} \equiv 0 \pmod{p} \qquad (10)$$

Складывая почленно (9) и (10), получим

$(p-a)^{r_1} \equiv -1 \pmod{p}$, откуда

$$(p-a)^{2r_1} \equiv 1 \pmod{p} \qquad (11).$$

Но $2r_1 < 2r$. Следовательно, сравнение (11) противоречит условию (6).

Теорема 1 доказана.

**Следствие.**

Число a будет первообразным корнем простого модуля p, тогда и только тогда, когда число p—a принадлежит к нечетному показателю $\frac{\varphi(p)}{2}$, где $\varphi(p)$ — функция Эйлера.

Пример. p=79, a=2.

$2^{\frac{\varphi(79)}{2}} = 2^{39} \equiv 1 \pmod{79}$. Число 2 принадлежит к нечетному показателю $39 = \frac{\varphi(79)}{2}$.

79—2=77.

77 — первообразный корень простого модуля 79.

Теорема 2. Числа a и p—a принадлежат к одному показателю по простому модулю $p \neq 2$ тогда и только тогда, когда показатель, которому принадлежит число a по модулю p есть число, кратное 4.

**Доказательство.**

1) Пусть числа a и p—a принадлежат к показателю n по простому модулю p. Покажем, что $n=4r$, где r — натуральное число. Предположим, что n не делится нацело на 4. Тогда n может быть либо нечетным, либо первой четности. Рассмотрим оба случая:

а) n — нечетное число. По условию $a^n \equiv 1 \pmod p$. В этом случае, согласно теореме 1, p—a принадлежит к показателю 2n, что противоречит условию;

б) $n=2r_1$, где $r_1$ — нечетное число.
Тогда $a^{2r_1} \equiv 1 \pmod p$ и согласно теореме 1 будем иметь $(p-a)^{r_1} \equiv 1 \pmod p$, что противоречит условию, ибо $r_1<n$.

2). Пусть a принадлежит к показателю $n=4r$. Покажем, что p—a принадлежит к тому же показателю n.

По условию $a^n = a^{4r} \equiv 1 \pmod p$. Используя условие, легко получить сравнение $p^{4r} - C_{4r}^1 p^{4r-1} a + \dots + a^{4r} \equiv 1 \pmod p$, откуда $(p-a)^{4r} \equiv 1 \pmod p$.

Предположим, что $(p-a)^{n_1} \equiv 1 \pmod p$, где $n_1<n$.

Число $n_1$ либо нечетное, либо первой четности, либо кратно 4

Первые две возможности исключаются теоремой 1.

Если бы $n_1 = 4r_1$, то $(p-a)^{4r_1} \equiv 1 \pmod p$, где $r_1<r$. Но тогда $p^{4r_1} - C_{4r_1}^1 p^{4r_1-1} a + \dots + a^{4r_1} \equiv 1 \pmod p$.

Откуда $a^{4r_1} = 1 \pmod p$, что противоречит условию.

Теорема 2 доказана.

**Следствие.**

p—a — первообразный корень простого модуля p тогда и только тогда, когда $\varphi(p)$ кратно 4 и a — первообразный корень простого модуля p.

Пример. $p=61$, $a=2$ — первообразный корень простого модуля 61.

$\varphi(61)=60=4 \cdot 15$, $61-2=59$.

59 — первообразный корень простого модуля 61.