9 июля

Лемма Гензеля

Обозначение: Будем обозначать степень, в которой простое число p входит в разложение n на простые множители, через $\mathrm{ord}_p(n)$.

Лемма Гензеля: Пусть a, b — различные целые числа, k — натуральное, а p — простое число, не делящее a. Если выполнено одно из условий 1) и 2), то $\mathrm{ord}_p(a^k - b^k) = \mathrm{ord}_p(a-b) + \mathrm{ord}_p(k)$.
1) $p \neq 2$ и $\mathrm{ord}_p(a-b) \geq 1$;
2) $p = 2$ и $\mathrm{ord}_p(a-b) \geq 2$.

Замечание: Иначе лемму Гензеля можно переформулировать так:
если $a \equiv b \pmod{p^\alpha}$ ($a \not\equiv 0 \pmod{p}$), α – максимальное число с этим свойством, то
а) при $p \neq 2$ выполнено $a^k \equiv b^k \pmod{p^{\alpha+s}}$, где $s \equiv \mathrm{ord}_p(k)$, и число $\alpha + s$ нельзя увеличить;
б) при $p = 2$ аналогичное верно только при $\alpha \geq 2$.

Доказательство: Предположим, что $a - b$ делится на p, причем a не делится на p.
а) Докажите, что $\mathrm{ord}_p(a^p - b^p) > \mathrm{ord}_p(a-b)$.
б) Докажите, что $\mathrm{ord}_p(a^s - b^s) = \mathrm{ord}_p(a-b)$, если s не делится на p.
в) Докажите, что $\mathrm{ord}_p(a^k - b^k) \geq \mathrm{ord}_p(a-b) + \mathrm{ord}_p(k)$.
г) Докажите, что если $p > 2$, то $\mathrm{ord}_p(a^p - b^p) = \mathrm{ord}_p(a-b) + 1$.
д) Докажите лемму Гензеля в случае, если выполнено условие 1).
е) Докажите лемму Гензеля в случае, если выполнено условие 2).

ЗАДАЧИ

1. В какой степени 5 входит в разложение числа $3^{10000} - 2^{10000}$ на простые множители?

2. Докажите, что показатель числа 2 по модулю 3^n равен $\varphi(3^n)$.

3. Решите в натуральных числах уравнение $3^x = 2^x y + 1$.

4. Найдите все четверки натуральных чисел (n, k, p, x), для которых $x > 2$, $n > 1$, p — простое и $x^n = p^k + 1$.

5. Какое наибольшее число нулей может быть среди шести последних цифр числа 2^n для $n > 100$?