Великая теорема Ферма. Правильное доказательство

Памяти МАМЫ

Противоречие: В равенстве $A^n=A^n+B^n$ [...=(A+B)R] число R имеет ДВА значения.

Все целые числа рассматриваются в системе счисления с простым основанием n>2.
Определения:
Степенным окончанием $A_{[t]}$ длиной t (t>1) цифр будем называть окончание $A'^{n^{t-1}}_{[t]}$ некоторого натурального числа $A=A'^{n^{t-1}}+Dn^t$, где A' – последняя цифра числа A.
Единичным окончанием $r_{[t]}$ числа r будем называть t-значное окончание равное 1.
Обозначения: A', A'', $A_{(t)}$ – первая, вторая, t-я цифра от конца в числе A;
A_2, A_3,$A_{[t]}$ – k-значное окончание числа A (т.е. $A_{[t]}=A \bmod n^t$); nn=n*n=n^2=n^2.
ВТФ доказывается для **базового** случая (см. http://vixra.org/abs/1707.0174):

L1°) **Лемма**. Цифра $A^n_{(t+1)}$ однозначно определяется окончанием $A_{[t]}$ (следствие из бинома Ньютона). То есть окончания A^n_2, $A^{n^2}_3$ и т.д. не зависят от цифры A'' и являются функцией лишь цифры A'.
L1.1°) Следствие: если $A_{[t+1]}=d^{n^t}_{[t+1]}$, где $d_2=e^n_2$, то
$A_{[t+2]}=e^{n^{t+1}}_{[t+2]}$ и $A^{n-1}_{[t+2]}=A'^{n-1}_{[t+2]}=1$.
L1.2°) При этом и $g^{n-1}_{[t+2]}=1$, где g есть сомножитель числа A, а g' – числа A'.
L1.3°) Если $C_{[t]}=C°_{[t]}$, $A_{[t]}=A°_{[t]}$, $B_{[t]}=B°_{[t]}$ и $C^n_{[t+1]}=A^n_{[t+1]}+B^n_{[t+1]}$, то и $C°^n_{[t+1]}=A°^n_{[t+1]}+B°^n_{[t+1]}$ (следствие из **L1.1°** и бинома Ньютона).

L2°) **Лемма**. t-значное окончание любого простого сомножителя числа R в равенстве $(A^n+B^n)_{[t+1]}=[(A+B)R]_{[t+1]}$, где $A_{[t]}=A^{n^{t-1}}_{[t]}$, $B_{[t]}=B^{n^{t-1}}_{[t]}$, $(A^{n^t}+B^{n^t})_{[t+1]}=C^{n^t}_{[t+1]}$, t>1, числа A и B взаимно простые и число A+B не кратно простому n>2, равно 1 –
следствие из: a) равенства $(CC^{n-1})_{[t+1]}=[(A+B)R]_{[t+1]}$, где $C_{[t]}=(A+B)_{[t]}=0$, b) определение степени и c) L1.2°.

***
Гипотетическое равенство Ферма имеет три эквивалентных формы:
1°) $C^n=A^n+B^n$ [...=(A+B)R=c^nr^n], $A^n=C^n-B^n$ [...=(C-B)P=a^np^n] и $B^n=C^n-A^n$ [...=(C-A)Q=b^nq^n], где при (ABC)'≠0 числа в парах (c, r), (a, p), (b, q) взаимно простые.

1.1°) Числа R, P, Q (без возможного сомножителя n) имеют единичные окончания с их наименьшей длиной в k цифр. Если, например, k=2, то наименьшее окончание будет 01.
1.2°) Следовательно, наименьшее единичное окончание y чисел r, p, q равно k-1 (цифр).

1.3°) Число U=A+B-C [=un^k] оканчивается на k нулей, даже если A', B' или C'=0.

1.4°) Если, например, C'=0, то число C оканчивается ровно на k нулей. При этом его особый сомножитель R оканчивается ровно на один ноль, который в число r не входит.
1.5°) Следовательно, в этом случае число A+B оканчивается nk-1 [>k] нулей.

L3°) **<u>Лемма.</u>** Если наименьшая длина единичного окончания у чисел r, p, q равна k-1 (и у чисел R, P, Q равна k), то k-значные степенно-степенные окончания чисел A и C-B, B и C-A, C и A+B, не кратных n, будут равны: $A'^{n\wedge\{k-1\}}$, $B'^{n\wedge\{k-1\}}$, $C'^{n\wedge\{k-1\}}$.
<u>Доказательство Леммы</u>. Пусть для начала k=2. Тогда из равенства $A+B-C=un^k$ (1.3°), с учетом 1° и L1°, мы находим равенства по двузначным окончаниям:
$C=c'^n$, $A=a'^n$, $B=b'^n \bmod n^2$, или $C_2=c'^n{}_2$, $A_2=a'^n{}_2$, $B_2=b'^n{}_2$.
Затем, если k>2, подставляем эти значения чисел A, B, C в левые части равенств 1°, учитываем свойство L1.1° и решаем систему уравнений $C^n=A+B$, $A^n=C-B$, $B^n=C-A$, относительно A, B, C. И т.д., пока не дойдем до значений $A'^{n\wedge\{k-1\}}$, $B'^{n\wedge\{k-1\}}$, $C'^{n\wedge\{k-1\}}$.

***

<u>Доказательство ВТФ</u>

2°) Пусть наименьшая длина единичного окончания среди чисел r, p, q будет у числа r и равна k-1 (в этом случае C'≠0). Тогда наименьшая длина единичного окончания у чисел R, P, Q не кратных n будет равна k. И, следовательно, число $U=A+B-C=un^k$.

Тогда, согласно L3°, в равенствах $C^n=A^n+B^n=(A+B)R=c^nr^n=CC^{n-1}$ (см. 1°) и

3°) $D=(A+B)^n{}_{[k+1]}=[(C-B)^n+(C-A)^n]_{[k+1]}=\{[(C-B)+(C-A)]T\}_{[k+1]}$ k-значные окончания чисел в парах C и A+B, A и C-B, B и C-A, C^{n-1} (=1) и $(A+B)^{n-1}$ (=1), R (=1) и T (=1) будут равными и степенно-степенными. Согласно Лемме L2°, каждый простой (и составной) сомножитель числа T имеет единичное окончание длиной не менее k цифр.
Но среди сомножителей числа T содержится и число r, причем строго в первой степени (ибо число [(C-B)+(C-A)] на r не делится, а числа r и D/r взаимно простые)!

И мы пришли к противоречию: в самом равенстве Ферма единичное окончание числа r имеет длину строго k-1 знаков, а в числе T – k знаков. Тем самым ВТФ доказана.

Мезос, 1 декабря 2017
++++++++++++++++